

Cisco Catalyst Center User Guide, Release 3.3.x

First Published: 2026-09-09

Last Modified: 2026-11-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **New and changed features in Catalyst Center** 1

PART I **Get Started** 7

CHAPTER 2 **Get Started with Catalyst Center** 9

- Catalyst Center overview 9
- Log in 9
- First-time setup 10
  - Log in to Catalyst Center for the first time 10
  - Complete the Quick Start workflow 13
    - Device credential information 15
  - Catalyst Center setup methods 17
    - Complete the express setup 18
    - Complete the standard setup 19
    - Complete the expert setup 22
- User profile roles and permissions 23
- Default home page 23
  - Main menu 24
  - Toolbar icons and help options 26
  - Default sections on the home page 27
  - Network and activity status icons 32
  - Interactive Help 33
  - Customize the home page 34
  - Action Required dialog box 34
- Reauthenticate Cisco.com and Smart Account credentials 34
- Catalyst Center journey map 35

View the remote support authorization dashboard 36
Use global search 37
Set the clock format to 12 hours or 24 hours 39
Apply light or dark appearance in Catalyst Center 39
Enable localization 39
Add a window to your favorites 40
Manage your favorites 41
Subscribe to Catalyst Center Insights 42

CHAPTER 3 **Configure Telemetry** 43
About telemetry settings 43
Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry 43
Criteria for enabling application telemetry on devices 45
Provision application telemetry settings 47
Enable application telemetry for wireless controllers 47
Update application telemetry to use a new cluster virtual IP address 49
Update device configuration using telemetry 50

PART II **Discover and Manage Network Inventory and Topology** 53

CHAPTER 4 **Discover Your Network** 55
Discovery overview 55
Discovery dashboard 56
Discovery prerequisites 56
Discovery credentials 57
Discovery credentials and Cisco ISE 61
Guidelines and limitations for Discovery credentials 62
Discovery credentials example 63
Preferred management IP addresses 63
Discovery configuration guidelines and limitations 64
Do Discovery 65
Discover your network using CDP 66
Discover your network using an IP address range or CIDR 68

Discover your network using LLDP 70
Manage Discovery jobs 73
Stop and start a Discovery job 73
Change credentials in a Discovery job 73
Clone a Discovery job 74
Delete a Discovery job 75

CHAPTER 5 **Manage Your Inventory** 77
About Inventory 78
Inventory and Cisco ISE authentication 79
Display information about your inventory 80
Display information about a device 86
Display information about a device interface 92
Display information about Ethernet ports 93
Manage port details 94
Manage per-device configurations for Cisco Catalyst Switches 96
View and edit the Layer 2 configuration of a device 99
View and edit Layer 3 configuration of a device 102
View and edit security configuration of a device 107
View and edit the network settings of a device 110
View and edit service configurations of a device 120
View and edit industrial configuration of a device 122
View and edit port configuration of a device 124
Inventory user interface enhancement 125
Manage user-defined fields 126
Create user-defined fields 126
Add user-defined fields to a device 127
Launch Topology map from Inventory 127
Types of devices in the Catalyst Center Inventory 128
Add devices to the Catalyst Center Inventory 128
Manage network devices 130
Add a network device 130
Update network device credentials 135
Security focus for network devices 139

View the integrity verification status of a device 140
View device certificate status 140
Manage compute devices 141
Add a compute device 141
Update compute device credentials 145
Manage Meraki dashboards 148
Integrate the Meraki dashboard 148
Update Meraki dashboard credentials 148
Manage Firepower Management Center 149
Integrate Firepower Management Center 149
Update Firepower Management Center credentials 150
Add a third-party device 151
Filter devices 154
Manage devices in the Inventory window 156
Assign an unprovisioned device to a site 156
Assign a provisioned device to a different site 157
Tag devices 158
Create a Network Device Group tag 159
Tag devices using rules 160
Edit device tags 160
Delete tags 161
Deal with SSH key verification errors 161
Configure the automatic acceptance of SSH key changes 162
Configure a REP ring for devices 162
Add a node to a REP ring for nonfabric deployment 164
Delete a node from a REP ring for nonfabric deployment 165
MRP ring for nonfabric deployment 166
View MRP ring topology overlay 167
View MRP ring status for nonfabric deployment 168
Parallel redundancy protocol 170
View the PRP topology status 171
Create port groups 172
Assign tags to ports 173
Port use information 173

Maintenance mode for devices 174
Schedule maintenance for devices 174
Manage maintenance schedule for devices 176
Remove a device from maintenance 176
Inventory Insights 177
Speed and duplex settings mismatch 177
VLAN mismatch 178
Manage system beacon 178
Device roles 179
Change the device role manually 180
Update a device management IP address 181
Update the device polling interval 181
Resynchronize device information 182
Delete a network device 183
Launch Command Runner (Inventory) 184
Troubleshoot device reachability issues using Run Commands 184
Use a CSV file to import and export device configurations 185
Import device configurations from a CSV file 186
Export device data 187
Export device credentials 188
Configuration drift of a device 189
View configuration drift of a device 190
Label configuration drift 192
Visibility and control of device configurations 193
Deploy your device configurations now or later 199
Preview and deploy your device configurations 200
Network provisioning prechecks 202
Replace a faulty device 205
Replace a faulty access point 211
Manage Out-of-band RMA device replacement 213
Limitations of the RMA workflow in Catalyst Center 214
Reboot an access point 216

CHAPTER 6 **Display Your Network Topology** 219

About topology 219
Display the topology of areas, sites, buildings, and floors 220
Filter devices on a topology map 220
Display device information 221
Display link information 223
Pin devices to a topology map 223
Save a topology map layout 224
Open a topology map layout 224
Share a topology map layout 225
Export the topology layout 225

PART III **Design Your Network** 227

CHAPTER 7 **Design the Network Hierarchy** 229
Network hierarchy 229
Design a new network hierarchy 231
Existing Cisco network hierarchies 231
Export your site hierarchy from Cisco Prime Infrastructure 232
Export your map archive from Cisco Prime Infrastructure 233
Import your site hierarchy to Catalyst Center 233
Import your map archive to Catalyst Center 234
Use an existing Ekahau network hierarchy 235
Export the Ekahau project from Catalyst Center 235
Import an Ekahau project to Catalyst Center 236
Import an Ekahau site survey to Catalyst Center 237
Export your network hierarchy from Catalyst Center 238
Export your site hierarchy from Catalyst Center 239
Export your map archive from Catalyst Center 239
Search the network hierarchy 240
Create the network hierarchy 240
Create, edit, and delete a site 240
Add, edit, and delete a building 242
Add, edit, and delete a floor 242
Add, edit, and delete an outdoor area 244

CHAPTER 8 **Work with Wireless 2D and 3D Floor Maps** 247

Floor maps overview 247

Heatmap overview 247

Add a floor with a map file 248

Floor map creation methods 249

Guidelines for image files to use in maps 249

Add a floor with a CAD map file 250

Add a floor with a non-CAD map file 251

Work with 2D maps 254

2D floor map devices and overlay objects 255

Work with APs on a floor map 256

Export APs from Cisco Prime Infrastructure and import into Catalyst Center 257

Add APs to a map 258

Add planned APs to a map 259

Autoplace planned APs on a map 261

Auto locate APs on a map 261

Assign actual APs to planned APs 265

Position an AP on a map 265

Reposition an AP on a map 269

Edit an AP 269

Edit multiple APs 272

Remove APs from a map 275

Work with sensors on a floor map 275

Add sensors to a map 275

Position sensors on a map 276

Reposition a sensor on a map 276

Remove sensors from a map 277

Add, edit, and remove coverage areas 277

Add, edit, copy, and remove openings 278

Add, edit, and remove location regions 279

Add, edit, and remove an inclusion region 279

Add, edit, and remove an exclusion region 280

Add, edit, and remove walls 280

Add, copy, edit, and remove shelving units 281
Add, edit, and remove markers 282
Add, edit, and remove GPS markers 283
Add, edit, and remove align points 283
View a 2D wireless heatmap 284
2D map toolbar 286
2D map view options 289
2D map navigation controls 292
About the AP icon and planned AP icon 292
View an unmanaged switch connected to managed APs 294
Filter device data on a floor 295
Identify wireless interferers on the floor map 296
Work with 3D maps 297
Configure floor map elements and overlays in 3D maps 298
Clone an AP 298
View a 3D wireless heatmap 299
3D wireless map toolbar 301
3D map view options 302
3D map navigation controls 304
Use first-person and third-person views for 3D wireless maps 308
Display details about APs and clients 310
Gain insights from a 3D wireless map 311
Run the wireless coverage optimizer 312
Create simulations for 3D wireless maps 313

CHAPTER 9 **Configure Network Settings** 317
Network settings overview 317
Configure the time zone for a site 318
Configure the message of the day 318
Add Cisco ISE or other AAA servers 319
Configure global network servers 321
Configure global device credentials 323
Configure global device credentials workflow 323
Add global CLI credentials 323

Add global SNMPv2c credentials 324
Add global SNMPv3 credentials 325
Add global HTTPS credentials 327
Assign device credentials to sites 329
Manage global device credentials 330
Apply device credentials to site devices 331
View the status of a device credential 333
Guidelines for editing global device credentials 334
Edit global device credentials 335
Delete device credentials 336
Update device credentials on devices 336
Configure IP address pools 337
Import IP address pools from an IP address manager 338
Import IP address pools from a CSV file 339
Reserve an IP address pool 339
Overlapping IP address pools 341
External IPAM integration 342
Notes and requirements for overlapping IP address pools 342
Troubleshooting overlapping IP address pools 343
Edit IP address pools 344
Delete IP address pools 345
Clone an IP address pool 345
Release IP address pools 345
View IP address pools 346
Configure service provider profiles 350
Configure global wireless settings 350
Customize the wireless network settings dashboard 351
Create SSIDs for an enterprise wireless network 351
Configure site-level overrides for an SSID for enterprise networks 360
Create Preauthentication Access Control Lists 362
Configure AAA server for an enterprise wireless network 364
Create SSIDs for a guest wireless network 366
Configure site-level overrides for an SSID for guest networks 376
Configure AAA server for a guest wireless network 378

Create SSID scheduler 380
Create a wireless interface 381
Design and provision VLAN groups for nonfabric deployments 381
Create a wireless radio frequency profile 383
Edit or delete a basic radio frequency profile 394
Clone a basic radio frequency profile 395
Prerequisites for configuring AI radio frequency profiles 396
Create an AI radio frequency profile 396
Edit an AI radio frequency profile 407
Delete an AI radio frequency profile 407
Clone an AI radio frequency profile 408
Configure AI-Enhanced RRM 409
Assign a location to an existing AI RF profile 412
Unassign a location from an existing AI RF profile 413
Upgrade a basic radio frequency profile to an AI radio frequency profile 416
Create an AP authorization list 417
Edit or delete an AP authorization list 419
Create an AP LSC renewal profile 419
Edit an AP LSC renewal profile 421
Delete AP LSC renewal profiles 421
Create an anchor group 422
Edit or delete an anchor group 424
AP profiles 424
Create an AP profile for Cisco IOS XE devices 425
Create an AP profile for Cisco AireOS devices 432
Edit or delete an AP profile 435
Create an AP power profile 436
Edit or delete an AP power profile 437
Provision a Cisco sensor SSID for nonfabric deployment 437
Manage backhaul settings 439
Create an antenna radio profile 440
Edit or delete an antenna radio profile 441
Cisco Connected Mobile Experiences integrations 441
Create Cisco CMX settings 442

About Cisco Spaces integration 444
Assign Cisco Spaces to sites 444
Monitor sites using Cisco Spaces 444
Configure a FlexConnect VLAN 445
Create an 802.11be profile 446
Edit or clone an 802.11be profile 448
Delete 802.11be profiles 449
About wireless mesh networks 449
Configure a certificate revocation check 451

CHAPTER 10 **Configure Network Profiles** 453
Network profiles overview 453
Create network profiles for assurance 453
Create network profiles for firewall 455
Create network profiles for routing 456
Create network profiles for switching 459
Create network profiles for wireless 460
Add SSIDs to a network profile 460
Add AP zones to a network profile 463
Add feature templates to a network profile 464
Add templates to a network profile 465
Overview of AP groups, flex groups, site tags, and policy tags 465
Custom AP group and flex group reuse examples 469
Custom policy tag reuse use case examples 472
Add AP groups, flex groups, site tags, and policy tags to a network profile 475
Configure additional interfaces for a network profile 478

PART IV **Configure and Maintain Network Devices** 481

CHAPTER 11 **Create Templates to Automate Device Configuration Changes** 483
About CLI Templates 483
Onboarding templates or day-zero templates 485
Deploy configurations on the network devices with day-n templates 485
Create projects 486

Create templates 486
Create a regular template 487
Blocked list commands 489
Sample templates 489
Create a composite template 489
Edit templates 491
Template simulation 492
Export templates 493
Import templates 493
Clone a template 494
Attach a CLI template to the network profiles 495
Provision CLI templates 495
Export projects 496
Import projects 497
Template variables 497
Variable binding 499
Special keywords 502
Associate templates to network profiles 504
Detect conflicts in a CLI template 506
Potential design conflicts detection between CLI template and service provisioning intent 506
Detect CLI template run-time conflict 507

CHAPTER 12 **Design Feature Templates** 509
Introduction to feature templates 509
Supported feature templates 510
Discover and create designs from a legacy device 510
Create a feature template for AAA RADIUS attributes 511
Create a feature template for advanced SSID 512
Create a feature template for Cisco CleanAir 517
Create a feature template for Dot11ax configuration 519
Create a feature template for Dot 11be status configuration 521
Create a feature template for event-driven RRM configuration 522
Create a feature template for Flex configuration 524
Create a feature template for Global IPv6 Configuration 525

Create a feature template for Multicast 526
Create a feature template for RRM FRA parameters 527
Create a feature template for RRM general parameters 528
Create a feature template for rogue general parameters 530

CHAPTER 13 Manage Software Images 533
About Software Image Management 533
Integrity Verification of software images 534
View software images 534
Use a recommended software image 538
Import a software image 539
Manage software image assignment for a device family 540
Schedule Image Update 542
Upload software images for devices in Install Mode 544
About standard software images 545
Mark a software image as standard 545
Manage the standard software image 547
Configure an image distribution server 548
Change the protocol order of an image distribution server 549
Add image distribution servers to sites 550
Provision a software image 551
Import the ISSU compatibility matrix 553
Upgrade a software image with ISSU or xFSU 554
List of device upgrade readiness prechecks 556
View image update status 557
View image update workflow 558
Auto flash cleanup 559

CHAPTER 14 Compliance Audit for Network Devices 561
Compliance overview 561
Compliance categories 562
Monitor the network compliance 567
Manage configuration compliance 569
Configure compliance settings 571

View compliance summary 572
Manual compliance run 574
Generate a compliance audit report for network devices 575
Acknowledge compliance violations 575
Synchronize startup and running configurations of a device 576
Fix compliance violations 577
Compliance behavior after device upgrade 578
Limitations in CLI template compliance 579

CHAPTER 15 **Run Diagnostic Commands on Devices** 581
Command Runner overview 581
Run diagnostic commands on devices 581

PART V **Provision Your Network** 583

CHAPTER 16 **Onboard and Provision Devices with Plug and Play** 585
Plug and Play provisioning overview 585
Plug and Play provisioning prerequisites 588
System certificate requirements for Plug and Play 590
DHCP controller discovery 590
DNS controller discovery 592
Plug and Play connect controller discovery 592
Plug and Play deployment guidelines 593
View devices 594
Add or edit a device 596
Add devices in bulk 597
Register or edit a virtual account profile 598
Add devices from a Smart Account 599
Provision a device with Plug and Play 601
Provision a switch or router device 602
Provision a wireless controller 606
Provision an AP or sensor device 609
Provision StackWise Virtual Link switch 612
Complete the provisioning process 613

Delete a device 614
Reset a device 614

CHAPTER 17 **Provision Wireless Devices** 617
Wireless device provisioning overview 617
About wireless devices and country codes 617
Configure regulatory activation for wireless controllers 618
Role-based access control 619
Prerequisites for provisioning a Cisco AireOS Controller 619
Provision a Cisco AireOS Controller 620
Configure Cisco Wireless Controller high availability 623
Prerequisites for configuring Cisco Wireless Controller high availability 623
Configure Cisco Wireless Controller HA 624
What happens during or after the high availability process is complete 625
Commands to configure and verify high availability 625
Disable high availability configured device in the existing deployment 626
Provision Cisco APs on day 1 627
Migrate APs from a Wireless Controller to another Wireless Controller 629
Reset APs 630
Enable ICMP ping on APs in FlexConnect mode 631
Day-zero workflow for Cisco AireOS Mobility Express APs 632
Configure and provision a Cisco Catalyst 9800 Series Wireless Controller 634
Cisco Catalyst 9800 Series Wireless Controller overview 634
Configure a Cisco Catalyst 9800 Series Wireless Controller in Catalyst Center 636
Software image upgrade support for Cisco Catalyst 9800 Series Wireless Controller 640
Configure high availability for the Cisco Catalyst 9800 Series Wireless Controller 641
Information about high availability 644
Commands to configure high availability on Cisco Catalyst 9800 Series Wireless Controllers 644
Commands to verify Cisco Catalyst 9800 Series Wireless Controllers high availability 645
N+1 high availability 645
Overview of N+1 high availability 645
Prerequisites for configuring N+1 high availability from Catalyst Center 646
Configure N+1 high availability from Catalyst Center 647
Mobility configuration overview 648

Mobility configuration workflow 649
Mobility configuration use cases 649
Configure mobility group 650
Configure AP Impersonation 652
About DTLS Ciphersuites 652
Configure Multiple DTLS Ciphersuites 653
About N+1 Rolling AP Upgrade 654
Workflow to Configure a Rolling AP Upgrade 654
Provision a Cisco Catalyst 9800 Series Wireless Controller 656
Day-zero workflow for Cisco Embedded Wireless Controller on Catalyst Access Points 662
Configure and provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches 664
Supported hardware platforms 664
Preconfiguration 665
Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches 666
Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches 668
Renew AP LSC for a wireless device 671
Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller 672
Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller 673
Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller 674
Configure per-device features for a Cisco Catalyst 9800 Series Wireless Controller 674
Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller 676
Customize table settings for Per-Device Configuration 677
Edit a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller 678
Clone a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller 679
Clone a Per-Device Configuration from another Cisco Catalyst 9800 Series Wireless Controller 680
Delete a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller 682
SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller 682
Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller 683
Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller 696
Create a remote LAN profile for a Cisco Catalyst 9800 Series Wireless Controller 704
Create a remote LAN policy for a Cisco Catalyst 9800 Series Wireless Controller 706
Create a policy tag for a Cisco Catalyst 9800 Series Wireless Controller 710
Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller 712

RF configurations for a Cisco Catalyst 9800 Series Wireless Controller 714
Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller 714
Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller 720
Create an RF tag for a Cisco Catalyst 9800 Series Wireless Controller 722
Create a multi-BSSID profile for a Cisco Catalyst 9800 Series Wireless Controller 724
Create a URWB network profile for a Cisco Catalyst 9800 Series Wireless Controller 725
Edit default RF settings for a Cisco Catalyst 9800 Series Wireless Controller 727
AP configurations for a Cisco Catalyst 9800 Series Wireless Controller 728
Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller 728
Configure global mesh parameters for a Cisco Catalyst 9800 Series Wireless Controller 744
Create a mesh PSK for a Cisco Catalyst 9800 Series Wireless Controller 746
Create a mesh profile for a Cisco Catalyst 9800 Series Wireless Controller 747
Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller 751
Create a flex profile for a Cisco Catalyst 9800 Series Wireless Controller 753
Create a site tag for a Cisco Catalyst 9800 Series Wireless Controller 758
Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller 759
Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller 761
Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller 761
Configure tag priority for a Cisco Catalyst 9800 Series Wireless Controller 762
Create static tag mapping for a Cisco Catalyst 9800 Series Wireless Controller 763
Create a location-based tag-mapping rule for a Cisco Catalyst 9800 Series Wireless Controller 764
Create a rule-based tag-mapping profile for a Cisco Catalyst 9800 Series Wireless Controller 766
Security configurations for a Cisco Catalyst 9800 Series Wireless Controller 768
Create a RADIUS server for a Cisco Catalyst 9800 Series Wireless Controller 768
Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller 770
Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller 771
Create a TACACS+ server group for a Cisco Catalyst 9800 Series Wireless Controller 772
Create an LDAP server for a Cisco Catalyst 9800 Series Wireless Controller 773
Create an LDAP server group for a Cisco Catalyst 9800 Series Wireless Controller 775
Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller 776
Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller 777
Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller 778
Configure global AAA parameters for a Cisco Catalyst 9800 Series Wireless Controller 779
Create a password policy for a Cisco Catalyst 9800 Series Wireless Controller 780

Configure RADIUS fallback for a Cisco Catalyst 9800 Series Wireless Controller 782
Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller 783
Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller 784
Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller 785
Create an IPv4 role-based ACL for a Cisco Catalyst 9800 Series Wireless Controller 787
Create an IPv4 extended ACL for a Cisco Catalyst 9800 Series Wireless Controller 789
Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller 792
Create an IPv6 role-based ACL for a Cisco Catalyst 9800 Series Wireless Controller 795
Create a MAC-based ACL for a Cisco Catalyst 9800 Series Wireless Controller 798
Create a local EAP profile for a Cisco Catalyst 9800 Series Wireless Controller 799
Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller 800
Configure advanced EAP for a Cisco Catalyst 9800 Series Wireless Controller 802
Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller 803
Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller 804
Create a guest user for a Cisco Catalyst 9800 Series Wireless Controller 806
Configure web authentication parameters for a Cisco Catalyst 9800 Series Wireless Controller 807
Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller 809
Configure CTS for a Cisco Catalyst 9800 Series Wireless Controller 813
Configure SXP for a Cisco Catalyst 9800 Series Wireless Controller 816
Create a CTS link configuration for a Cisco Catalyst 9800 Series Wireless Controller 817
Create an SXP AP profile for a Cisco Catalyst 9800 Series Wireless Controller 818
Configure rogue policies for a Cisco Catalyst 9800 Series Wireless Controller 820
Create a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller 823
Configure client exclusion policies for a Cisco Catalyst 9800 Series Wireless Controller 826
Configure LSC provision parameters for a Cisco Catalyst 9800 Series Wireless Controller 827
Create an LSC provisioning entry for a Cisco Catalyst 9800 Series Wireless Controller 829
Create a key chain for a Cisco Catalyst 9800 Series Wireless Controller 830
Configure AP certificate policy for a Cisco Catalyst 9800 Series Wireless Controller 832
Create an AP certificate policy using MAC address for a Cisco Catalyst 9800 Series Wireless Controller 832
Create an AP certificate policy using serial number for a Cisco Catalyst 9800 Series Wireless Controller 834
Global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller 835
Configure CleanAir for a Cisco Catalyst 9800 Series Wireless Controller 835

Configure high throughput parameters for a Cisco Catalyst 9800 Series Wireless Controller 838
Configure media parameters for a Cisco Catalyst 9800 Series Wireless Controller 841
Configure Air Time Fairness for a Cisco Catalyst 9800 Series Wireless Controller 844
Create an Air Time Fairness policy for a Cisco Catalyst 9800 Series Wireless Controller 845
Configure network parameters for a Cisco Catalyst 9800 Series Wireless Controller 846
Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller 851
Configure RRM on the 6-GHz band for a Cisco Catalyst 9800 Series Wireless Controller 855
Configure RRM on the 5-GHz band for a Cisco Catalyst 9800 Series Wireless Controller 859
Configure RRM on the 2.4-GHz band for a Cisco Catalyst 9800 Series Wireless Controller 865
Configure RRM FRA parameters for a Cisco Catalyst 9800 Series Wireless Controller 871
Configure global wireless parameters for a Cisco Catalyst 9800 Series Wireless Controller 873
Configure load balancing for a Cisco Catalyst 9800 Series Wireless Controller 876
Configure band selection for a Cisco Catalyst 9800 Series Wireless Controller 877
Configure optimized roaming for a Cisco Catalyst 9800 Series Wireless Controller 879
Configure high-density parameters for a Cisco Catalyst 9800 Series Wireless Controller 880
Add a preferred call for a Cisco Catalyst 9800 Series Wireless Controller 882
Configure RFID for a Cisco Catalyst 9800 Series Wireless Controller 883
Configure cellular steering for a Cisco Catalyst 9800 Series Wireless Controller 884
Configure 6-GHz client steering for a Cisco Catalyst 9800 Series Wireless Controller 885
Configure mDNS for a Cisco Catalyst 9800 Series Wireless Controller 886
Create an mDNS service definition for a Cisco Catalyst 9800 Series Wireless Controller 887
Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller 889
Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller 890
Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller 892
Create an mDNS flex profile for a Cisco Catalyst 9800 Series Wireless Controller 893
Configure multicast for a Cisco Catalyst 9800 Series Wireless Controller 894
Configure IGMP snooping for a Cisco Catalyst 9800 Series Wireless Controller 895
Configure MLD snooping for a Cisco Catalyst 9800 Series Wireless Controller 896
Configure PIM and multicast-routing for a Cisco Catalyst 9800 Series Wireless Controller 897
Create a VRF to RP address map for a Cisco Catalyst 9800 Series Wireless Controller 898
Create wireless broadcast and non-IP multicast for a Cisco Catalyst 9800 Series Wireless Controller 899
Configure location for a Cisco Catalyst 9800 Series Wireless Controller 900
Configure country codes for a Cisco Catalyst 9800 Series Wireless Controller 901

Configure Cisco DNA integration settings for a Cisco Catalyst 9800 Series Wireless Controller 902
Configure AP policy for a Cisco Catalyst 9800 Series Wireless Controller 903
Create a device authentication serial number for a Cisco Catalyst 9800 Series Wireless Controller 904
Create a device authentication MAC Address for a Cisco Catalyst 9800 Series Wireless Controller 905
Configure wireless geolocation settings for a Cisco Catalyst 9800 Series Wireless Controller 906
Service configurations for a Cisco Catalyst 9800 Series Wireless Controller 907
Create a service template for a Cisco Catalyst 9800 Series Wireless Controller 907
Create a policy map for a Cisco Catalyst 9800 Series Wireless Controller 908
Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller 910
Create a custom application for a Cisco Catalyst 9800 Series Wireless Controller 913
Create an exporter for a Cisco Catalyst 9800 Series Wireless Controller 915
Create a flow monitor for a Cisco Catalyst 9800 Series Wireless Controller 916
Configure EoGRE global parameters for a Cisco Catalyst 9800 Series Wireless Controller 917
Create an EoGRE gateway for a Cisco Catalyst 9800 Series Wireless Controller 918
Create an EoGRE domain for a Cisco Catalyst 9800 Series Wireless Controller 919
Create an EoGRE tunnel profile for a Cisco Catalyst 9800 Series Wireless Controller 920
Configure media stream for a Cisco Catalyst 9800 Series Wireless Controller 922
Create a media stream profile for a Cisco Catalyst 9800 Series Wireless Controller 923
Create a guest LAN profile for a Cisco Catalyst 9800 Series Wireless Controller 925
Create a guest LAN map for a Cisco Catalyst 9800 Series Wireless Controller 926
Add an excluded client for a Cisco Catalyst 9800 Series Wireless Controller 928
Configure ThousandEyes for a Cisco Catalyst 9800 Series Wireless Controller 929
Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller 930
Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller 930
Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller 934
Create a VLAN group profile for a Cisco Catalyst 9800 Series Wireless Controller 935
Create a port channel interface for a Cisco Catalyst 9800 Series Wireless Controller 935
Create loopback interface for a Cisco Catalyst 9800 Series Wireless Controller 937
Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller 939
Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller 940
Configure the wireless management interface for a Cisco Catalyst 9800 Series Wireless Controller 941
Configure discovery protocols for a Cisco Catalyst 9800 Series Wireless Controller 943

Network settings for a Cisco Catalyst 9800 Series Wireless Controller 944
Configure DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller 944
Create an IPv4 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller 946
Create an IPv6 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller 948
Configure DHCP persistence for a Cisco Catalyst 9800 Series Wireless Controller 950
Configure HTTP and HTTPS for a Cisco Catalyst 9800 Series Wireless Controller 951
Configure general SNMP parameters for a Cisco Catalyst 9800 Series Wireless Controller 953
Configure SNMP wireless traps for a Cisco Catalyst 9800 Series Wireless Controller 954
Add an SNMP community string for a Cisco Catalyst 9800 Series Wireless Controller 955
Create SNMPv3 user group for a Cisco Catalyst 9800 Series Wireless Controller 956
Create an SNMPv3 user for a Cisco Catalyst 9800 Series Wireless Controller 958
Create an SNMP host for a Cisco Catalyst 9800 Series Wireless Controller 959
Create an NTP server profile for a Cisco Catalyst 9800 Series Wireless Controller 961
Create an authentication key profile for a Cisco Catalyst 9800 Series Wireless Controller 962
Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller 963
Create a static route for a Cisco Catalyst 9800 Series Wireless Controller 963
Administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller 965
Configure device administration settings for a Cisco Catalyst 9800 Series Wireless Controller 965
Configure device FTP/SFTP/TFTP settings for a Cisco Catalyst 9800 Series Wireless Controller 966
Configure user administration settings for a Cisco Catalyst 9800 Series Wireless Controller 967
Configure AP upgrade settings for a Cisco Catalyst 9800 Series Wireless Controller 968
Inter-Release Controller Mobility introduction 969
Guest anchor configuration and provisioning process 970
Prerequisites for configuring IRCM on a Cisco controller device 971
Configuring IRCM on a Cisco AireOS Controller and a Cisco Catalyst 9800 Series Wireless Controller 972
Prerequisites for provisioning a Meraki device 973
Provision a Meraki device 973
Provision remote teleworker devices 975
Remote teleworker deployment overview 975
Create a remote teleworker site 977

CHAPTER 18 **Provision a Routing Profile** 981
Provision a router 981

VPC Inventory collection 983

CHAPTER 19 **Provision Firewall Profiles** 985

Provision a firewall Threat Defense device 985

Provision a firewall Adaptive Security Appliance device 987

CHAPTER 20 **Provision a LAN Underlay** 989

LAN automation 989

Prerequisites for provisioning a network through LAN automation 990

Provision a network through LAN automation 991

Peer Device in LAN automation use case 997

Check the LAN automation status 999

Create a link between interfaces 999

Delete a link between interfaces 1000

Edit hostname and loopback IP address of LAN automated devices 1001

Manage devices in strict discovery mode 1002

CHAPTER 21 **Provision SD-Access LISP Fabric Network** 1005

Cisco SD-Access zero-trust security solution 1005

Zero-Trust Overview dashboard 1006

Day-zero view of the Zero-Trust Overview dashboard 1006

Get started with SD-Access zero-trust workplace journey 1008

Day-n view of Zero-Trust Overview dashboard 1009

Modify SD-Access zero-trust workplace journey 1011

About fabric networks 1012

Fabric sites 1012

Transits 1013

Fabric readiness, image compatibility, and compliance checks 1013

Fabric Health Check 1014

Fabric scale checks 1015

Fabric site updates 1015

Role-based access control for Cisco SD-Access 1017

Add a fabric site 1018

Move a fabric site 1020

Configure a fabric site 1021
Add a device to a fabric 1022
Remove a device from a fabric 1025
Add a device as a border node 1027
Configure LISP Pub/Sub 1030
Reconfigure a fabric 1031
Create an IP transit 1032
Create an SD-Access transit 1033
Configure an authentication template for the fabric site 1035
Configure ports within the fabric site 1036
Configure wireless SSIDs for fabric networks 1038
Configure a wireless mesh access point in a fabric 1039
Configure security service insertion on a fabric site 1039
Virtual networks 1040
Create a Layer 3 virtual network 1040
Create a Layer 2 virtual network 1042
Associate Layer 3 virtual networks to fabric sites 1043
Create anycast gateways 1044
Configure Cisco ISE for fabric AP MACsec on edge nodes 1049
Extranet policy 1049
Extranet policy management 1050
Guidelines for configuring an extranet policy 1050
Create an extranet policy 1051
Edit an extranet policy 1051
Delete an extranet policy 1052
Configure a fabric zone 1052
Create a fabric site and fabric zones 1053
Create a fabric zone within a fabric site 1054
Associate Layer 3 virtual networks to fabric zones 1055
Associate Layer 2 virtual networks to fabric zones 1056
Associate anycast gateways to fabric zones 1057
Configure an extended node device 1058
Configure an extended node 1059
Upgrade an extended node to a policy-extended node 1061

Delete an extended node 1063
Configure a REP ring topology for extended nodes and policy-extended nodes 1063
View REP ring status 1065
Delete a REP ring 1066
Add a node to a REP ring 1066
Delete a node from a REP ring 1067
Configure supplicant-based extended nodes 1068
Steps to configure a supplicant-based extended node 1068
Replace a faulty port 1070
Configure Cisco Identity Services Engine to onboard supplicant-based extended node 1071
Configure a port channel 1074
Create a port channel 1074
Update a port channel 1076
Delete a port channel 1076
Multicast 1077
Configure multicast 1077
Edit BGP AS number for a fabric site 1079
Shared wireless controllers for multiple fabric sites 1080
Configure a shared wireless controller for multiple fabric sites 1083
Prepare network profiles for wireless controller sharing 1084
Add a shared wireless controller to a remote fabric site 1085
Edit remote fabric sites for a shared wireless controller 1086
Remove a shared wireless controller from a fabric 1086

CHAPTER 22 **Provision Campus Networks** 1089
Campus networks 1089
Manage networks 1090
Create a network 1091
Manage configuration profiles 1092
Create a configuration profile for switching device group 1093
Create port configuration profiles for switching device groups 1093
Create configuration profiles for wireless controllers 1096
Learn configuration profiles from a wireless controller 1097
Manage switching device groups 1099

Learn configuration profiles from a switch 1101
Provision a switching device group 1103
Manage devices 1105
Assign wireless controllers to an existing network 1106
Assign configuration profiles to a wireless controller 1107
Edit configuration profile assignment for a wireless controller 1108
Delete configuration profile from a wireless controller 1109
Configure per-device overrides for wireless controller configuration profiles 1110
Compare device configurations 1111

CHAPTER 23 **Provision Services** 1113
Applications 1113
About Application Visibility 1113
Application Visibility view 1114
Configure CBAR cloud 1117
Enable or disable CBAR cloud 1118
Enable CBAR on network devices 1119
Disable CBAR on network devices 1120
Enable Application Telemetry 1120
Disable Application Telemetry 1121
Update the protocol pack on a CBAR-enabled device 1122
Reconfigure CBAR on network devices 1123
Applications and application sets 1124
Unidirectional and bidirectional application traffic 1124
Custom applications 1124
Discovered applications 1125
Favorite applications 1125
Configure applications and application sets 1126
Change application settings 1126
Create a server name-based custom application 1127
Create an IP address and port-based custom application 1127
Create a URL-based custom application 1128
Edit or delete a custom application 1129
Mark an application as favorite 1130

Create a custom application set 1130
Edit or delete a custom application set 1131
Discover unclassified applications 1131
Application Visibility service support for the Catalyst Center Traffic Telemetry Appliance 1132
Discover Infoblox applications 1132
Edit or delete a discovered application 1133
Application hosting 1134
About application hosting 1134
Install or update the application hosting service package 1135
Prerequisites for application hosting 1135
View device readiness to host an application 1136
Application hosting readiness checks 1137
View devices and status for a selected application 1138
Add an application 1139
Automatic download of the ThousandEyes Enterprise Agent application 1139
Update an application 1140
Start an application 1140
Stop an application 1141
View applications hosted on a device 1141
Install an application using application hosting 1142
Install applications in bulk using a CSV file 1143
Uninstall an application from a Cisco Catalyst 9300 device 1144
Edit an application configuration in a Cisco Catalyst 9300 device 1145
Delete an application 1145
Download application logs 1146
Download device tech support logs 1146
Application hosting on Cisco Catalyst 9100 Series Access Points 1146
About application hosting on Cisco Catalyst 9100 Series Access Points 1146
Application hosting workflow to install and manage USB applications on Cisco Catalyst 9100 Series Access Points 1147
View installed hosting applications on Cisco Catalyst 9100 Series Access Points 1148
Uninstall an application from a Cisco Catalyst 9100 device 1149
Delete an application from a Cisco Catalyst 9100 device 1149
Configure a site-to-site VPN 1150

Create a site-to-site VPN 1150
Edit a site-to-site VPN 1151
Delete a site-to-site VPN 1151
Configure Cisco Umbrella 1151
About Cisco Umbrella 1152
Role-based access control settings for Cisco Umbrella 1152
Configure Cisco Umbrella with Catalyst Center 1152
Add the Umbrella dashlet 1153
View the Umbrella service statistics dashboard 1154
Prerequisites for provisioning Cisco Umbrella on network devices 1154
Provision Cisco Umbrella on network devices 1155
Disable Cisco Umbrella on network devices 1157
Update the Cisco Umbrella configuration on network devices 1158
Create secure tunnel 1159
Configure secure tunnel 1159
Security service insertion for SD-Access 1161
Service insertion sites 1161
Prechecks to enable a service insertion site on day zero 1162
Enable a service insertion site 1164
Edit a service insertion site 1165
Delete a service insertion site 1169
Configure traffic steering contracts 1169
Secure Equipment Access 1170
Set up the Cisco IoT Dashboard 1171
Log in to the Cisco IoT Dashboard 1171
Configure Secure Equipment Access 1172
Generate an API key 1174
Integrate Cisco Cyber Vision Center with Catalyst Center 1175
Manage Cyber Vision Centers 1175
Deploy sensor for Cyber Vision Center 1176

PART VI **Configure Policies** 1179

CHAPTER 24 **Configure Group-Based Access Control Policies and Analytics** 1181

Group-based access control 1181
Group-Based Access Control Policy dashboard 1182
Group-based access control policies 1183
Policy creation overview 1186
Create a security group 1186
Edit a security group 1187
Delete a security group 1188
Synchronization of security groups between Catalyst Center and Cisco ISE 1188
Create an access contract 1189
Edit an access contract 1190
Delete an access contract 1191
Synchronization of access contracts between Catalyst Center and Cisco ISE 1192
Create group-based access control policy 1192
Update a group-based access control policy based on traffic flows 1194
Synchronization of policies between Catalyst Center and Cisco ISE 1195
Cisco Group-Based Policy Analytics 1195
About Cisco Group-Based Policy Analytics 1195
Install Group-Based Policy Analytics 1196
Hardware and software compatibility 1196
Understand connectors 1199
Initial configuration of Cisco Group-Based Policy Analytics 1199
Explore groups and endpoints 1200
Multiple groups to multiple groups 1200
Single group to multiple groups 1201
Single group to single group 1202
Access contracts 1205
Date and time selector 1206
Use Search 1207
Role-Based Access Control 1208

CHAPTER 25 **Configure IP-Based and URL-Based Access Control Policies** 1209
IP-based access control policies 1209
Workflow to configure an IP-based access control policy 1210
Configure global network servers 1210

Create an IP Network Group 1212
Edit or delete an IP Network Group 1212
Create an IP-based access control contract 1212
Edit or delete an IP-based access control contract 1213
Create an IP-based and URL-based access control policy 1214
Edit or delete an IP-based and URL-based access control policy 1215

CHAPTER 26 Configure Application Policies 1217
Application policies overview 1217
CVD-based settings in application policies 1218
Site scope 1218
Business-relevance groups 1218
Consumers and producers 1219
Marking, queuing, and dropping treatments 1219
Service provider profiles 1222
Queuing profiles 1224
Processing order for devices with limited resources 1225
Policy drafts 1227
Policy scheduling 1228
Policy Versioning 1228
Original policy restore 1229
Stale application policies 1229
Application policy guidelines and limitations 1230
Manage application policies 1231
Prerequisites 1231
Create an application policy 1231
View application policy information 1234
Edit an application policy 1235
Save a draft of an application policy 1236
Deploy an application policy 1237
Cancel a policy deployment 1238
Delete an application policy 1238
Clone an application policy 1238
Restore an application policy 1239

Reset the default CVD application policy 1240
Display application policy history 1240
Roll back to a previous policy version 1241
Manage queuing profiles 1241
Create a queuing profile 1241
Edit or delete a queuing profile 1242
Manage application policies for WAN interfaces 1243
Customize service provider profile SLA attributes 1243
Assign a service provider profile to a WAN interface 1244

CHAPTER 27 Configure Traffic-Copy Policies 1247
Traffic copy policies 1247
Sources, destinations, and traffic copy destinations 1247
Guidelines and limitations of traffic copy policy 1248
Workflow to configure a traffic copy policy 1249
Create a traffic copy destination 1249
Edit or delete a traffic copy destination 1250
Create a traffic copy contract 1250
Edit or delete a traffic copy contract 1250
Create a traffic copy policy 1251
Edit or delete a traffic copy policy 1251

CHAPTER 28 Configure Rule-Based Compliance Policies 1253
Rule-based compliance policies 1253
Create a rule-based compliance policy 1254
Create rule-based compliance policy rules 1254
Add a condition to the compliance policy rule 1255
Example: Block Options 1259
Example Conditions and Actions: NTP Server Redundancy 1261
Add a variable to the policy rule 1261
Assign a policy to sites 1263
Export a compliance policy as XML from Cisco Prime Infrastructure and import into Catalyst Center 1263
Export a rule-based compliance policy from Catalyst Center and import it into another Catalyst Center 1264

CHAPTER 29 **Configure Traffic Steering Policies** 1265

Traffic steering policy overview 1265

Traffic steering policies 1266

Create a traffic steering policy on day zero 1267

Create a traffic steering policy on day n 1267

Edit a traffic steering policy 1268

Delete traffic steering policies 1269

Deploy traffic steering policies 1270

Traffic steering contracts 1270

Create a traffic steering contract 1270

Edit or duplicate a traffic steering contract 1272

Delete traffic steering contracts 1273

PART VII **Monitor and Troubleshoot Your Network** 1275

CHAPTER 30 **Enable Advanced Feature Trials** 1277

Advanced Features trial overview 1277

Enable the Network Bug Identifier trial 1277

Enable the Security Advisories trial 1278

Enable the Field Notices trial 1278

CHAPTER 31 **Cisco AI Endpoint Analytics** 1281

Cisco AI Endpoint Analytics overview 1281

Key features of Cisco AI Endpoint Analytics 1282

FIPS compliance 1283

Set up Cisco AI Endpoint Analytics in Catalyst Center 1283

Install software updates 1284

Connect and enable data sources 1284

Endpoint telemetry sources 1287

Cisco AI Endpoint Analytics overview window 1287

Cisco Talos Intelligence 1288

Integrate Cisco AI Endpoint Analytics with Cisco Talos Intelligence through app activation 1289

Integrate Cisco AI Endpoint Analytics with Cisco Talos Intelligence using cloud authentication 1290

Publish authorization attributes to Cisco ISE 1292
Trust Analytics 1293
Customize impact level 1294
Configure reset alert 1295
Endpoint Purge Policies 1295
Create a Purge Policy 1296
Configure endpoint subnet inspection 1297
Endpoint Inventory 1297
Export Cisco AI Endpoint Analytics data 1298
Filter endpoints 1299
Attribute Glossary 1300
Register endpoints 1301
Edit registered endpoints 1302
Delete registered endpoints 1302
Trust Score 1302
Trust Scores for endpoints 1303
Endpoint Attribute Conflict 1306
NAT Mode Detection 1307
Endpoints with concurrent MAC addresses connected to Cisco Catalyst 9000 Series devices 1308
Initial Trust Score assessment using Posture and authentication values from Cisco ISE 1308
Trust Scores for endpoints with random and changing MAC addresses 1309
Sensor scans to check for open ports and credential vulnerabilities 1310
View and manage Trust Scores for endpoints 1312
Control endpoint spoofing 1317
Profiling rules 1318
Rule prioritization 1318
Filter profiling rules 1319
View updated profiling rules 1319
System rules 1319
Automatic system rule updates for endpoint profiling 1320
Custom rules 1321
Logic and conditions for profiling rules 1321
Create a custom rule 1322
Edit a custom rule 1322

Delete a custom rule 1323
Export and import custom profiling rules across deployments using APIs 1323
Cisco AI rules for smart grouping 1324
New profiling suggestions for similar endpoints in your network 1324
Import profiling rules 1326
Export profiling rules 1326
Hierarchy 1327
Create category and subcategory 1327
Edit a category or subcategory 1328
Delete endpoint types from category 1328
Reassign endpoint types from category 1328
Delete a category 1329

CHAPTER 32 **Troubleshoot Network Devices Using Network Reasoner** 1331
Network Reasoner overview 1331
Validate Cisco SD-Access migration using the MRE workflow 1331
Troubleshoot high CPU use 1333
Troubleshoot a power supply failure 1335
Troubleshoot a downed interface 1336
Troubleshoot network connectivity 1337
Troubleshoot IP connectivity of a device 1338
Troubleshoot wireless clients using the MRE workflow 1339
Troubleshoot wireless APs using the MRE workflow 1340
Troubleshoot unmonitored devices using the MRE workflow 1341
Troubleshoot HA on Cisco Wireless Controller using the MRE workflow 1341

CHAPTER 33 **Identify Network Bugs** 1345
Network bug identifier tool overview 1345
Scan the network for bugs 1346
Scan Catalyst Center for bugs 1347

CHAPTER 34 **Identify Network Security Advisories** 1349
Security advisories overview 1349
Prerequisites 1350

View security advisories 1350
Schedule a security advisories scan 1352
CLI commands invoked for security advisories 1353
Rescan the network to identify security advisories 1353
Hide and unhide devices from an advisory 1354
Hide and unhide advisories from a device 1355
Add notification for a security advisory knowledge bundle 1355
View security advisories in the inventory 1356
Live Protect Shields overview 1357
Shield deployment sidebar 1358
Live Protect Shields permissions 1359
Complete the Live Protect Shields prerequisites 1359
Open the Live Protect Shields view 1360
Deploy a Live Protect Shield 1360
Switch between Monitoring and Enforcing modes 1361
Deploy a newer shield version 1362
Deactivate a Live Protect Shield 1362
View events and customize the table view 1363
Add a match pattern 1363
Define AND/OR for the match pattern 1364
Edit the match pattern 1365
Delete the match pattern 1365

CHAPTER 35 **Identify Network Field Notices** 1367
Field Notices identifier tool overview 1367
View Field Notices 1367

CHAPTER 36 **Generate the Root Cause Analysis File from Catalyst Center** 1369
Support Bundle overview 1369
Collect and upload provisioning failure root cause analysis data 1369

PART VIII **Manage Catalyst Center** 1371

CHAPTER 37 **Build and Deploy Workflows** 1373

Catalyst Center workflow navigation 1373
Discover devices 1374
AP Refresh workflow 1375
Enable application hosting on switches 1378
Enable IoT services 1380
Enable IoT services on Cisco Catalyst 9100 Series Access Points 1380
Manage IoT applications 1381
AP configurations in Catalyst Center 1382
Configure APs 1382
Schedule recurring events for APs 1400
Configure APs using existing templates 1403
Replace a device 1407
Switch refresh 1413
Create a remote support authorization 1415
Create an event notification 1416
Configure Remote LAN 1420
Configure Parallel Redundancy Protocol in a fabric site 1423
Delete PRP configuration 1425
Edit PRP channel 1426

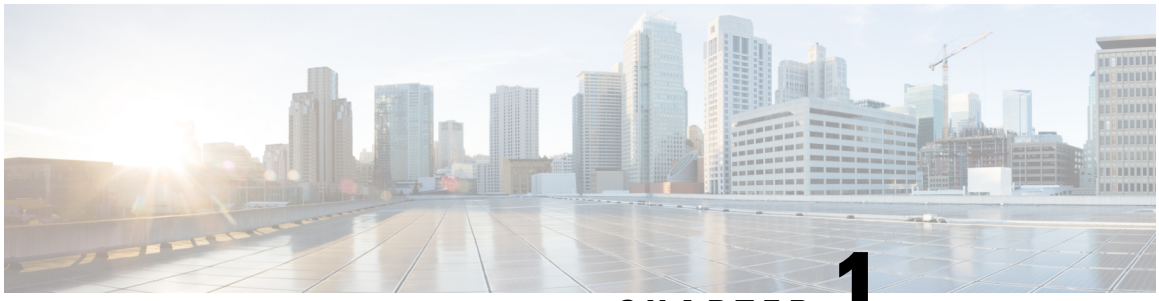
CHAPTER 38 **Wireless Network Configuration Use Cases** 1427
Wireless network configuration use case 1427
Wireless controller management use cases 1427
WLAN profile and policy profile configuration 1427
Wi-Fi 7 configuration use case 1430
Enable the Wi-Fi 7 configuration 1430
High availability use cases 1432
Configure Cisco Wireless Controller HA 1433
Configure Cisco Wireless Controller N+1 HA 1434
Wireless mobility use cases 1435
Configure wireless mobility 1435
Configure anchor and foreign wireless mobility 1438
AP management use cases 1441
AP configuration 1442

AP refresh 1442
Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning 1442
Automated tagging for flapping APs 1445
Configure ROW APs 1445
Configure wireless mesh network 1446
AP migration from a wireless controller to another wireless controller 1448
AP replacement using RMA workflow 1448
Onboard APs using PnP for non-intent-based deployments 1448
Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers 1450
Standardize complete configuration for wireless controllers on day zero 1450
Standardize partial configuration for wireless controllers on day zero 1451
Manage configurations for a wireless controller on day n 1452

CHAPTER 39 **Manage Energy on Your Network** 1455
Overview 1455
Manage energy on network devices 1455
Use the Energy Management dashboard 1457
Generate a report of energy management for network devices 1458
View energy consumption of network devices 1459
Carbon emissions of network devices 1460
View energy savings 1461
Compare energy across sites 1462

CHAPTER 40 **Troubleshoot Catalyst Center Using Data Platform** 1467
About Data Platform 1467
View or update Collector configuration information 1468
View data retention settings 1469
View pipeline status 1469

CHAPTER 41 **Proactive Remediation for Discovered Issues** 1471
Proactive remediation for discovered issues 1471
Approve or decline a corrective action 1471



CHAPTER 1

New and changed features in Catalyst Center

This table summarizes the new and changed features in Catalyst Center 3.3.2 and tells you where they are documented.

Table 1: New and changed features in Catalyst Center 3.3.2

Feature	Description
Shared wireless controller for multiple fabric sites	Catalyst Center now supports sharing a Cisco Catalyst 9800 Series Wireless Controller across multiple SD-Access fabric sites. **Note** This feature is in beta. A wireless controller can be shared across a maximum of 16 fabric sites. You can select eligible remote fabric sites, validate network profile compatibility, resolve configuration conflicts, and prepare site-specific wireless intent before deployment. Refer to Shared wireless controllers for multiple fabric sites, on page 1080 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

This table summarizes the new and changed features in Catalyst Center 3.3.1 and tells you where they are documented.

Table 2: New and changed features in Catalyst Center 3.3.1

Feature	Description
Decouple templates configuration from network profile	If you want to configure one or a few devices with specific configurations that do not apply to the rest of the devices at the same site, you can provision the CLI template without associating it with a network profile. The compliance check is skipped if you provision the template without associating it with a network profile. Refer to Provision CLI templates, on page 495
Enhancements to application hosting	Catalyst Center supports multi-architecture app packages across CPU architectures such as x86_64 and aarch64. Refer to Install an application using application hosting, on page 1142

Feature	Description
Enhancements to delete a REP ring.	If any device in the REP ring is unreachable, you cannot delete the ring. Use Catalyst Center to rediscover the REP ring so you can remove unreachable devices and then delete the ring. Refer to Delete a REP ring, on page 1066
Enhancements to MRP monitoring	When the link between two devices goes down in an MRP ring, Catalyst Center indicates the affected MRP Ring node. Refer to View MRP ring topology overlay, on page 167
Enhancements to the AP configuration workflow	The **Configure Access Points** workflow is enhanced for improved usability. Refer to Configure APs, on page 1382, Schedule recurring events for APs, on page 1400, and Configure APs using existing templates, on page 1403.
Enhancements to per-device configurations for Cisco Catalyst Switches in Catalyst Center	Catalyst Center supports these enhancements for Cisco Catalyst Switches: • Configuration of QoS, BFD, OSPF, and AAA attributes in the per-device configurations. • Per-device configuration support for fabric devices. Refer to View and edit service configurations of a device, on page 120, View and edit Layer 3 configuration of a device, on page 102, View and edit the network settings of a device, on page 110, and Manage per-device configurations for Cisco Catalyst Switches, on page 96.
Enhancements to Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers are enhanced to support new and updated configurations for Cisco IOS XE Release 26.2.1. Refer to Configure ThousandEyes for a Cisco Catalyst 9800 Series Wireless Controller, on page 929, Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 720, Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 728, Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 683, Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777, Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 696, Configure global wireless parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 873, and Edit default RF settings for a Cisco Catalyst 9800 Series Wireless Controller, on page 727.
Enhancements to port configuration profiles for Cisco Catalyst Switches in campus networks workflow	The configuration profiles for Cisco Catalyst Switches has been enhanced to support additional profiles for port configurations. Refer to Create port configuration profiles for switching device groups, on page 1093.
Enhancements to REP ring configuration	You can configure REP ring with MACsec encryption. Refer to Configure a REP ring for devices, on page 162.

Feature	Description
Enhancements to the scheduling experience in the Visibility and Control of Configurations workflow	Catalyst Center streamlines the scheduling experience in the Visibility and Control of Configurations workflow: • Configure scheduling and preview from one page. • Enable configuration preview using the **Preview** check box. Refer to Visibility and control of device configurations, on page 193, Preview and deploy your device configurations, on page 200, and Deploy your device configurations now or later, on page 199.
Enhancements to the wireless controller provisioning workflow in campus networks	Catalyst Center supports these enhancements for provisioning wireless controllers in a campus network: • Associate configuration profiles to multiple wireless controllers. • Create new configuration profile for wireless controllers. • Support for additional configurations for wireless controller configuration profile. • Configure and review device overrides for wireless controller configuration profiles. Refer to Manage configuration profiles, on page 1092, Create configuration profiles for wireless controllers, on page 1096, Assign configuration profiles to a wireless controller, on page 1107, and Configure per-device overrides for wireless controller configuration profiles, on page 1110.
Enhancements to the switching provisioning workflow in campus networks	Catalyst Center supports these features for provisioning switching devices in a campus network. • Configuration of Industrial configuration profile. • Configuration of device-level overrides for configuration profile attributes. Refer to Provision a switching device group, on page 1103.
Enhancements to the wireless SSID creation workflow for enterprise and guest wireless networks	The wireless SSID creation workflow has these enhancements for enterprise and guest wireless networks: • The **Associate SSID to Wireless Network Profile** window is enhanced. • Under **Auth Key Management**, **FT + 802.1x** and **802.1x-SHA256 (802.1X-SHA2)** options are supported for the **GCMP256** encryption. Refer to Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

Feature	Description
Live Protect	Live Protect validates security shields that protect Cisco products without requiring device reloads or service interruptions. You can deploy security shields in two modes: • Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Enforce (Protecting) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire the security shields, enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risks until the software upgrades or patches are deployed. Refer to Live Protect Shields overview, on page 1357.
Regulatory activation for wireless controllers	Catalyst Center supports regulatory activation for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in nonfabric deployment. When the APs associated with a wireless controller are unable to obtain a country code through standard geolocation or proximity methods, the AP radios are not operational. Catalyst Center can use the regulatory activation file obtained from the Meraki dashboard to resolve the country code on these APs. Refer to Configure regulatory activation for wireless controllers, on page 618.
RMA device support	Catalyst Center provides RMA support for Cisco IE3500 and IE3100 Rugged Series switches.
Support for automatic service insertion site updates for edge node and border node addition and deletion in fabric sites	Catalyst Center now automatically updates a service insertion site when an edge node or border node is added to or deleted from the corresponding fabric site. Refer to Manage devices associated with a service insertion site, on page 1168.
Support for Cisco TrustSec (CTS) data download over HTTPS	Catalyst Center allows using HTTPS for CTS policy and data download. You can enable or disable this option in Catalyst Center while configuring the ISE servers under **Design** > **Network Settings** > **Servers**. Refer to Add Cisco ISE or other AAA servers, on page 319.

Feature	Description
Support for Cisco Wireless 9177D, 9177E, and 9177I Series Access Points	Catalyst Center supports the Cisco Wireless 9177D, 9177E, and 9177I Series Access Points. You can configure these APs with Wi-Fi 7 for Cisco IOS XE Release 26.2.1 or later, enable bridge and mesh roles, and use dual-band (XOR) capability to operate slot 2 in either 5-GHz or 6-GHz radio mode. **Note** When configuring these APs using the **Configure Access Points** workflow, you cannot set radio parameters for slot 2 in the **Configure 6 GHz Radio Parameters** window. Use the **Configure Dual-Band (XOR) Radio Parameters** window to manage these settings. Refer to Configure APs, on page 1382, Schedule recurring events for APs, on page 1400, Enable the Wi-Fi 7 configuration, on page 1430, and Supported hardware platforms, on page 664.
Support for MACsec encryption in AP profile for Cisco IOS XE devices	Catalyst Center supports MACsec encryption and automatic MACsec configuration in AP profiles for Cisco IOS XE devices. The **MACsec Encrypted** toggle button is applicable for: • Cisco Catalyst 9000 Series Switches running Cisco IOS XE Release 17.18.3 or 26.1.1. • Wireless controllers running Cisco IOS XE Release 26.1.1 or later. **Note** Catalyst Center does not support MACsec encryption for fabric sites that contain Cisco Catalyst 9350 Series Smart Switches. The **Auto-Secure MACsec** toggle button is supported on applicable Wi-Fi 7 APs and Cisco Catalyst 9350 Series Smart Switches running Cisco IOS XE Release 26.2.1 or later. **Note** This configuration is supported only in nonfabric deployments on Cisco Catalyst 9350 Series Smart Switches. It is not supported in fabric deployments. Refer to Configure management settings for an AP profile for Cisco IOS XE devices, on page 425.
Support for MACsec encryption for fabric APs	For the INFRA_VN virtual network, Catalyst Center supports MACsec encryption of AP uplink traffic for supported APs during anycast gateway configuration. Refer to Create anycast gateways, on page 1044.

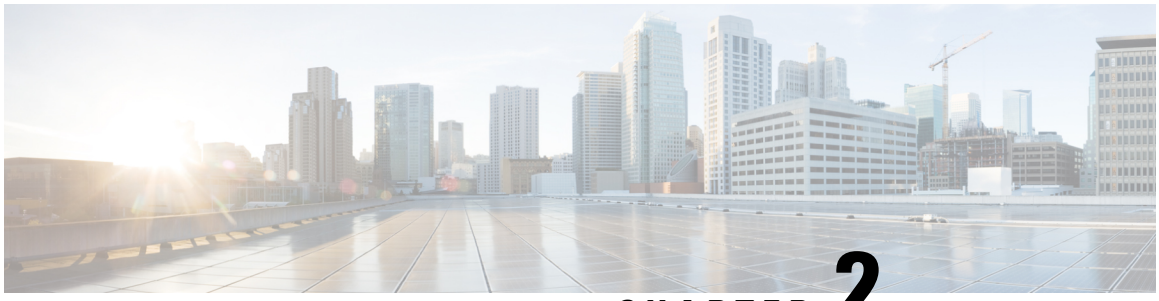
Feature	Description
Support for security service insertion for SD-Access over HTTPS	Security service insertion for SD-Access is enhanced to support Cisco TrustSec (CTS) policy and data download over HTTPS: • To enable service insertion on a fabric site on day zero, you must enable CTS policy and data download over HTTPS for the site. • To disable CTS policy and data download over HTTPS for a site configured as a service insertion site, you must delete the security service insertion configuration. **Note** If you upgrade to this release from an earlier release, CTS policy and data download over HTTPS is disabled by default. You must enable CTS policy and data download over HTTPS on the service insertion site after you upgrade to ensure ongoing security service insertion operations on day *n*. Refer to Service insertion sites, on page 1161, Prechecks to enable a service insertion site on day zero, on page 1162 and Add Cisco ISE or other AAA servers, on page 319.
Support for Rule-Based Compliance (RBC) Remediation	Catalyst Center supports the remediation of violations generated by Rule-Based Compliance (RBC) policies, allowing you to automatically fix non-compliant devices by applying user-defined CLI commands.
Ultra Reliable Wireless Backhaul (URWB) network profile support for wireless controller.	You can create a Ultra Reliable Wireless Backhaul (URWB) network profile for a wireless controller and provision it. Refer to Create a URWB network profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 725
Rule-Based Compliance Remediation	Rule-based compliance remediation helps you manage rule-based violations. You can filter remediable and non-remediable issues and apply fixes through a preview or schedule them for deployments. Refer to Fix compliance violations, on page 577, and Add a condition to the compliance policy rule, on page 1255.



PART I

Get Started

- Get Started with Catalyst Center, on page 9
- Configure Telemetry, on page 43



CHAPTER 2

Get Started with Catalyst Center

- Catalyst Center overview, on page 9
- Log in, on page 9
- First-time setup, on page 10
- User profile roles and permissions, on page 23
- Default home page, on page 23
- Reauthenticate Cisco.com and Smart Account credentials, on page 34
- Catalyst Center journey map, on page 35
- View the remote support authorization dashboard, on page 36
- Use global search, on page 37
- Set the clock format to 12 hours or 24 hours, on page 39
- Apply light or dark appearance in Catalyst Center, on page 39
- Enable localization, on page 39
- Add a window to your favorites, on page 40
- Manage your favorites, on page 41
- Subscribe to Catalyst Center Insights, on page 42

Catalyst Center overview

Using Catalyst Center, you can centrally manage your network. You can easily and quickly design, provision, and apply policies. You gain network visibility across the entire environment by using the Catalyst Center GUI. You can use network insights to improve performance.

Log in

Access Catalyst Center by entering its network IP address in your browser. Review the list of compatible browsers in the *Cisco Catalyst Center Release Notes*. This IP address connects to the external network and is configured during the Catalyst Center installation. For more information about installing and configuring Catalyst Center, see the *Cisco Catalyst Center Installation Guide*.

You can configure the idle session timeout as an administrator option. See "Account Lockout" in the *Cisco Catalyst Center Administrator Guide* for steps to configure the idle session timeout.

Procedure

Step 1 Enter an address in your web browser address bar in this format: *server-ip*. The *server-ip* represents the IP address or the hostname of the server where you installed Catalyst Center.

https://*server-ip*

Example: https://192.0.2.1

Depending on your network setup, you might need to update your browser configuration to trust the Catalyst Center server security certificate. Doing this ensures a secure connection between your client and Catalyst Center.

Step 2 Enter the Catalyst Center username and password assigned to you by the system administrator. Catalyst Center displays its home page.

If your user ID has the SUPER-ADMIN-ROLE and you are the first to log in with this role, a first-time setup wizard appears instead of the home page.

Step 3 You can log out by clicking your displayed username in the top-right corner, then selecting **Log Out**.

First-time setup

This section provides instructions for setting up Catalyst Center for first-time production use after you've completed the installation and configuration of your Catalyst Center appliance. It covers the initial GUI access, admin user setup, and Catalyst Center setup options.

To set up Catalyst Center for first-time production use, you'll need to:

1. Log in to Catalyst Center for the first time and create a new admin user. For instructions, refer to Log in to Catalyst Center for the first time, on page 10.
2. Complete the Catalyst Center setup using either the Quick Start workflow or one of the enhanced setup methods. For instructions, refer to Complete the Quick Start workflow, on page 13 and Catalyst Center setup methods, on page 17.

Log in to Catalyst Center for the first time

After you have installed and configured the Catalyst Center appliance, follow these steps to log in to its GUI for the first time. You will log in for the first time as the admin superuser (with the username admin and the SUPER-ADMIN-ROLE assigned).

Note Use a compatible, HTTPS-enabled browser when accessing Catalyst Center. For more information, refer to "Compatible browsers" in the "Complete First-Time Setup" chapter of the *Cisco Catalyst Center Installation Guide*.

Before you begin

Make sure that you have this information on hand, so you can log in to Catalyst Center:

- The *admin* superuser username and password that you specified while configuring your Catalyst Center appliance.
- The information described in "Required first-time setup information" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.

Procedure

Step 1 Access the Catalyst Center GUI:

a) After the Catalyst Center appliance reboot completes, do one of these tasks:

- If you used the browser-based configuration wizard: Click **Open Catalyst Center Virtual Appliance** on the last page of the wizard.
- If you used the Maglev Configuration wizard: Launch a compatible, HTTPS-enabled browser. Then enter the host IP address to access the Catalyst Center GUI, using **`HTTPS://`** and the IP address of the Catalyst Center GUI, which appears at the end of the configuration process.

One of these messages appears (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

b) Click **Advanced** to continue.

One of these messages appears:

- Google Chrome:

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
 by your computer's
 operating system. This may be caused by a misconfiguration or an attacker intercepting your
 connection.
```

- Mozilla Firefox:

```
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates.
Firefox does not trust GUI-IP-address because its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

These messages appear because the controller uses a self-signed certificate. For information about how Catalyst Center uses certificates, refer to "Certificate and private key support" in the *Cisco Catalyst Center Administrator Guide*.

c) Do one of these tasks to continue:

- Google Chrome: Click the **Proceed to** *GUI-IP-address* **(unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

Step 2 Log in to Catalyst Center:

a) After the Catalyst Center login window opens, do one of these configuration wizard completion tasks:

- With Maglev configuration wizard completion and selection of the **Start using DNAC pre manufactured cluster** option, enter the admin username (**admin**) and password (**P@ssword9**).
- With Maglev configuration wizard completion and selection of the **Start configuration of DNAC in advanced mode** option, enter the admin username (**admin**) and password that you configured for your Catalyst Center appliance.
- With Install configuration wizard completion, enter the admin username (**admin**) and paste the password (**P@ssword9**) that you copied from the last wizard window.
- With Advanced Install configuration wizard completion, enter the admin username (**admin**) and password that you set when you configured your Catalyst Center appliance.

b) Click **Log In**.

Step 3 Configure a new admin user, as a security measure:

a) Enter this information:

- **Roles**: Confirm that the `SUPER-ADMIN` role is already set.
- **New Username**: Enter the admin user username.
- **Email**: Enter the admin user email address.
- **New Password** and **Confirm Password**: Enter the admin user password. Ensure that this password complies with the password requirements. Refer to "Password requirements" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.

Note Changing the default password is critical to network security, especially when the people who set up the appliance are not the same people who will serve as its administrators.

b) Click **Submit**.

Catalyst Center logs you out.

Step 4 Log back in to Catalyst Center:

a) Click **Log In**.
b) Enter the new admin username and password that you just configured.
c) Click **Log In**.

You are prompted to authenticate using your cisco.com credentials, which are used to register software downloads and receive system communications.

Step 5 Click **Authenticate**.

Note If you don't want to authenticate now, click **Skip** instead.

Step 6 Confirm that an activation code is listed in the **Activate your device** pop-up window, then click **Next**.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

Step 7 Review the documents and click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Catalyst Center.

What to do next

You can continue with the first-time setup by completing either the Quick Start workfow or one of the enhanced setup methods. For more information, refer to Complete the Quick Start workflow, on page 13 and Catalyst Center setup methods, on page 17.

Complete the Quick Start workflow

Complete this workflow to discover the devices that Catalyst Center will manage and enable the collection of telemetry from those devices.

Note Alternatively, you can set up Catalyst Center using one of the enhanced setup methods. For more information, refer to Catalyst Center setup methods, on page 17.

After you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts.

Before you begin

Ensure that you meet these prerequisites:

- Initial setup: You successfully logged in to Catalyst Center for the first time and created a new admin user. For more information, refer to Log in to Catalyst Center for the first time, on page 10.
- Required information: You have the information described in "Required first-time setup information" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide* on hand.

  This includes:

  - User access planning: A list of users who need access to the system, including their roles, unique passwords, and privilege settings.
  - Service integration (optional): If you plan to use an IPAM server or Cisco Identity Services Engine (ISE), have the relevant URL and login information ready.

Procedure

Step 1 In the **Quick Start Overview** slider, select **Let's Do it**.

Step 2 In the **Discover Devices: Provide IP Ranges** screen, enter this information and then select **Next**:

- The name for the device discovery job.
- The IP address ranges of the devices you want to discover. Select + to enter additional ranges.
- Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, refer to Preferred management IP addresses, on page 63.

Step 3 In the **Discover Devices: Provide Credentials** screen, enter the information described in Device credential information, on page 15 for the type of credentials you want to configure and then select **Next**.

Step 4 In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then select **Next**.

You can enter the site's information manually or select the location you want to use in the provided map.

Step 5 In the **Enable Telemetry** screen, check the network components that you want Catalyst Center to collect telemetry for and then select **Next**.



Note If both the **Enable Telemetry** and **Disable Telemetry** options are grayed out, this indicates that either devices are not capable of supporting telemetry or devices are running an OS version that does not support telemetry enablement.

Step 6 In the **Summary** screen, review the settings that you have entered and then do one of these tasks:

- If you want to make changes, select the appropriate **Edit** link to open the relevant screen.
- If you're happy with the settings, select **Start Discovery and Telemetry**. Catalyst Center validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.

  Catalyst Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

A message appears at the top of the home page after the Quick Start workflow has completed.

What to do next

- Select **View Discovery** to open the **Discovery** page and confirm that the devices in your network have been discovered.
- Select the **Go to Network Settings** link to open the **Device Credentials** page. From here, you can verify that the credentials you entered previously have been configured for your site.
- Select the **View Activity Page** link to open the **Tasks** page and view any tasks (such as a weekly scan of the network for security advisories) that Catalyst Center has already scheduled to run.
- Select the **Workflow Home** link to access guided workflows that will help you set up and maintain your network.

Device credential information

This table describes the information you need to enter in the **Discover Devices: Provide Credentials** screen when completing the Quick Start workflow.

Table 3: Description of device credential fields

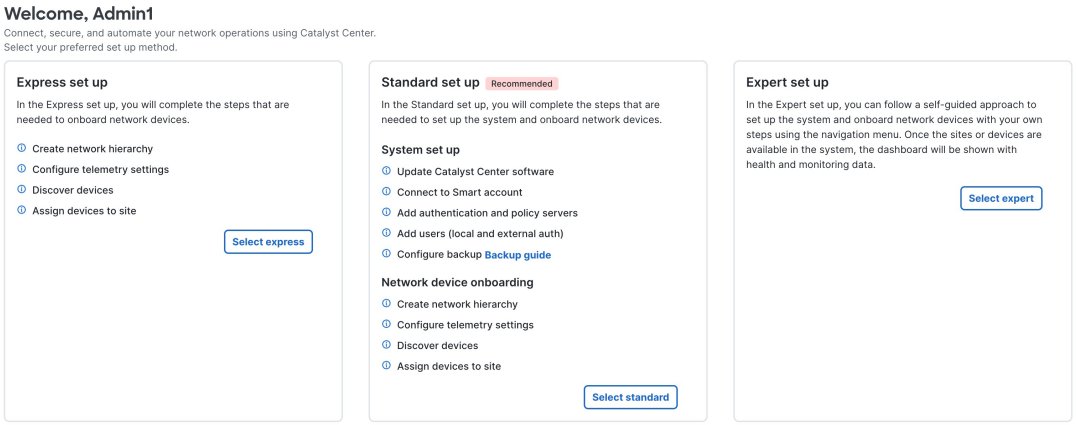
Field	Description
CLI (SSH) Credentials	
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network. The password you enter must be at least eight characters long.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
SNMP Credentials: SNMPv2c Read tab **Note** Catalyst Center does not support SNMPv2c credentials when FIPS mode is enabled. You'll need to enter SNMPv3 credentials instead. For more information regarding FIPS mode, refer to "Configure the primary node using the Maglev wizard" in the "Configure the Appliance Using the Maglev Wizard" chapter of the *Cisco Catalyst Center Installation Guide*.	
Name/Description	Name or description of the SNMPv2c read community string.
Community String	Read-only community string password used only to view SNMP information on the device.
SNMP Credentials: SNMPv2c Write tab	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
SNMP Credentials: SNMPv3	
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	Security level that SNMP messages require: • **No Authentication, No Privacy** (noAuthnoPriv): Does not provide authentication or encryption. • **Authentication, No Privacy** (authNoPriv): Provides authentication, but does not provide encryption. • **Authentication and Privacy** (authPriv): Provides both authentication and encryption. **Note** When FIPS mode is enabled, Catalyst Center only supports **Authentication and Privacy** mode.

Field	Description
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either **Authentication and Privacy** or **Authentication, No Privacy** is set as the authentication mode: • **SHA**: HMAC-SHA authentication. • **MD5**: HMAC-MD5 authentication. **Note** Catalyst Center does not support this authentication type when FIPS mode is enabled.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Choose one of the following privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices. **Note** For the Catalyst Center third-generation appliance: • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance. For Catalyst Center on ESXi: • Privacy types AES192 and AES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages are exchanged with devices supported with AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
NETCONF	
Port	The NETCONF port that Catalyst Center should use in order to discover wireless controllers that run Cisco IOS-XE.

Catalyst Center setup methods

When you log in for the first time, the Quick Start workflow automatically starts. To view the enhanced setup methods, exit the Quick Start workflow and go to the default home page. The default home page displays the available setup methods.



If you have SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE permissions, you can set up Catalyst Center using one of these methods:

- Express setup: This setup helps you onboard network devices. For instructions, see Complete the express setup method.
- Standard setup: This recommended setup helps you set up the system and onboard network devices. For instructions, see Complete the standard setup method.

- Expert setup: This self-directed setup allows you to independently set up the system and onboard network devices. We recommend this option for expert users only. For instructions, see Complete the expert setup, on page 22.

Note If you start one setup method and later decide that you'd prefer to use a different setup method, you can change your selected method. Return to the default home page and click **Select <setup method name>** to start a different setup method.

Complete the express setup

Follow these steps to set up Catalyst Center using the express setup method.

Before you begin

Ensure that you successfully completed Log in to Catalyst Center for the first time, on page 10.

Procedure

Step 1 From the home page, click **Select express**.

The express setup method starts and opens the **Design** > **Network Hierarchy** page. The **Express set up** slide-in pane displays the steps to complete this setup method.

Tip

- We recommend that you complete the steps in the order that they are presented.
- You can view the relevant page for any step by clicking **Go to this step**.
- You can close the **Express set up** slide-in pane at any time by clicking **Exit**. In the dialog box, click **Exit** again.
- After you complete at least one of the listed steps, you can reopen this slide-in pane by clicking **Express set up** in the top-right portion of Catalyst Center.
- You can view all completed steps by scrolling to the end of this slide-in pane and opening the **<Number of> steps completed** section. To mark a completed step as incomplete, check the **Mark as complete** check box for that step. The step becomes incomplete, and the progress bar updates to reflect this change.

Step 2 Complete the create network hierarchy step.

a) On the **Design** > **Network Hierarchy** page, create the network hierarchy—including areas, buildings, and floors.

For instructions, refer to Design the Network Hierarchy, on page 229.

b) Under **Create network hierarchy**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that one of four steps is complete.

Step 3 Complete the telemetry settings step.

a) Under **Configure telemetry settings**, click **Go to this step**.
b) On the **Design** > **Network Settings** page for **Telemetry**, configure the required telemetry settings for telemetry data collection.

   For instructions, refer to Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 43.

c) Under **Configure telemetry settings**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that two of four steps are complete.

Step 4 Complete the discover devices step.

a) Under **Discover devices**, click **Go to this step**.

   The onboard devices workflow begins.

b) Discover your devices by completing the onboard devices workflow.

   For instructions, refer to Do Discovery, on page 65.

c) Under **Discover devices**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that three of four steps are complete.

Step 5 Complete the assign devices to site step.

a) Under **Assign devices to site**, click **Go to this step**.
b) On the **Provision** > **Inventory** page, assign your devices to the relevant sites.

   For instructions, refer to Assign an unprovisioned device to a site, on page 156 and Assign a provisioned device to a different site, on page 157.

c) Under **Assign devices to site**, check the **Mark as complete** check box for this step.

   The progress bar updates and indicates that four of four steps are complete. A completion message summarizes the number of created sites and discovered devices.

Step 6 Click **Launch home page** to complete the express setup of Catalyst Center.

The home page displays when the express setup of Catalyst Center is complete.

Note The system may take some time to display discovered devices on the home page.

Complete the standard setup

Follow these steps to set up Catalyst Center using the standard setup method.

Before you begin

Ensure that you successfully completed Log in to Catalyst Center for the first time, on page 10.

Procedure

Step 1 From the home page, click **Select standard**.

The standard setup method starts and opens the **System** > **Software Management** page. The **Standard set up** slide-in pane displays the steps to complete this setup method.

Tip

- We recommend that you complete the steps in the order that they are presented.
- You can view the relevant page for any step by clicking **Go to this step**.
- You can close the **Standard set up** slide-in pane at any time by clicking **Exit**. In the dialog box, click **Exit** again.
- After you complete at least one of the listed steps, you can reopen this slide-in pane by clicking **Standard set up** in the top-right portion of Catalyst Center.
- You can view all completed steps by scrolling to the bottom of this slide-in pane and opening the **<Number of> steps completed** section. To mark a completed step as incomplete, check the **Mark as complete** check box for that step. The step becomes incomplete, and the progress bar updates to reflect this change.

Step 2 Complete the update the Catalyst Center software step.

a) On the **System** > **Software Management** page, update the Catalyst Center software to the latest recommended version.

For instructions, refer to the *Cisco Catalyst Center Upgrade Guide*.

b) Under **Update Catalyst Center software**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that one of nine steps is complete.

Step 3 Complete the connect to smart account step.

a) Under **Connect to Smart account**, click **Go to this step**.

b) On the **Smart Account** page, connect your Cisco Smart Account to your Smart Licensing account.

For instructions, refer to "Configure Smart Account" in the *Cisco Catalyst Center Administrator Guide*.

c) Under **Connect to Smart account**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that two of nine steps are complete.

Step 4 Complete the add authentication and policy servers step.

a) Under **Add authentication and policy servers**, click **Go to this step**.

b) On the **Authentication and Policy Servers** page, add either a Cisco Identity Services Engine (Cisco ISE) or AAA server.

Catalyst Center uses AAA servers for user authentication or Cisco ISE for both user authentication and access control. For instructions, refer to "Configure authentication and policy servers" in the *Cisco Catalyst Center Administrator Guide*.

c) Under **Add authentication and policy servers**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that three of nine steps are complete.

Step 5 Complete the add users step.

a) Under **Add users (local and external auth)**, click **Go to this step**.

b) On the **User Management** page, add the required users, so they can access Catalyst Center.

For instructions, refer to "Create an internal user" in the *Cisco Catalyst Center Administrator Guide*.

c) If your network requires using an external server for authentication and authorization of external users, enable external authentication.

For instructions, refer to "Configure external authentication" in the *Cisco Catalyst Center Administrator Guide*.

d) Under **Add users (local and external auth)**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that four of nine steps are complete.

Step 6 Complete the configure backup step.

a) Under **Configure backup**, click **Go to this step**.

b) On the **System** > **Backup & Restore** page, configure a remote server to back up your automation and Assurance data from Catalyst Center and connect a remote server to restore automation and Assurance data from Catalyst Center.

For instructions, refer to "Configure the location to store backup files" and "Restore data from backups" in the *Cisco Catalyst Center Administrator Guide*.

c) Under **Configure backup**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that five of nine steps are complete.

Step 7 Complete the create network hierarchy step.

a) Under **Create network hierarchy**, click **Go to this step**.

b) On the **Design** > **Network Hierarchy** page, create the network hierarchy—including areas, buildings, and floors.

For instructions, refer to Design the Network Hierarchy, on page 229.

c) Under **Create network hierarchy**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that six of nine steps are complete.

Step 8 Complete the telemetry settings step.

a) Under **Configure telemetry settings**, click **Go to this step**.

b) On the **Design** > **Network Settings** page for **Telemetry**, configure the required telemetry settings for telemetry data collection.

For instructions, refer to Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 43.

c) Under **Configure telemetry settings**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that seven of nine steps are complete.

Step 9 Complete the discover devices step.

a) Under **Discover devices**, click **Go to this step**.

The onboard devices workflow begins.

b) Discover your devices by completing the onboard devices workflow.

For instructions, refer to Do Discovery, on page 65.

c) Under **Discover devices**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that eight of nine steps are complete.

Step 10 Complete the assign devices to site step.

a) Under **Assign devices to site**, click **Go to this step**.

b) On the **Provision** > **Inventory** page, assign your devices to the relevant sites.

For instructions, refer to Assign an unprovisioned device to a site, on page 156 and Assign a provisioned device to a different site, on page 157.

c) Under **Assign devices to site**, check the **Mark as complete** check box for this step.

The progress bar updates and indicates that nine of nine steps are complete. A completion message summarizes the number of created sites and discovered devices.

Step 11 Click **Launch home page** to complete the standard setup of Catalyst Center.

The home page displays when the standard setup of Catalyst Center is complete.

Note The system may take some time to display discovered devices on the home page.

Complete the expert setup

Follow these steps to set up Catalyst Center using the expert setup method.

Before you begin

Note We recommend that only expert network administrators use this setup method. This method does not provide detailed setup instructions. The express and standard setup methods provide step-by-step instructions. For more information, see Catalyst Center setup methods, on page 17.

Before you begin

Ensure that you successfully completed Log in to Catalyst Center for the first time, on page 10.

Procedure

Step 1 From the home page, click **Select expert**.

Step 2 In the **Expert set up** dialog box, click **Ok** to continue.

Step 3 Set up Catalyst Center as required for your network.

For general instructions on setting up your network, consider referring to this information:

- Design the Network Hierarchy, on page 229
- Discover Your Network, on page 55
- Manage Your Inventory, on page 77

After you complete device discovery, the default home page is displayed—indicating that you completed the expert setup of Catalyst Center.

User profile roles and permissions

Catalyst Center supports role-based access control (RBAC). Your user role determines your permissions. Catalyst Center has these three main default user roles:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE, and
- OBSERVER-ROLE.

The SUPER-ADMIN-ROLE allows comprehensive access and supports creating and assigning custom roles in the Catalyst Center GUI. The user roles for NETWORK-ADMIN-ROLE and OBSERVER-ROLE provide limited access.

You can create access groups that limit access to certain network sites. An access group combines a role and a site. You can log in to a specific access group at any time.

Catalyst Center supports these default access groups:

- **NW-ADMIN_Global** - For global access to the role NW-ADMIN
- **OBSERVER_Global** - For global access to the role OBSERVER, and
- **SUPER-ADMIN_Global** - For global access to the role SUPER-ADMIN.

The behavior of Catalyst Center features depends on the user role and site specified in the access group. For more information, see *Configure site-based, role-based access control* in the *Cisco Catalyst Center Administrator Guide*.

Default home page

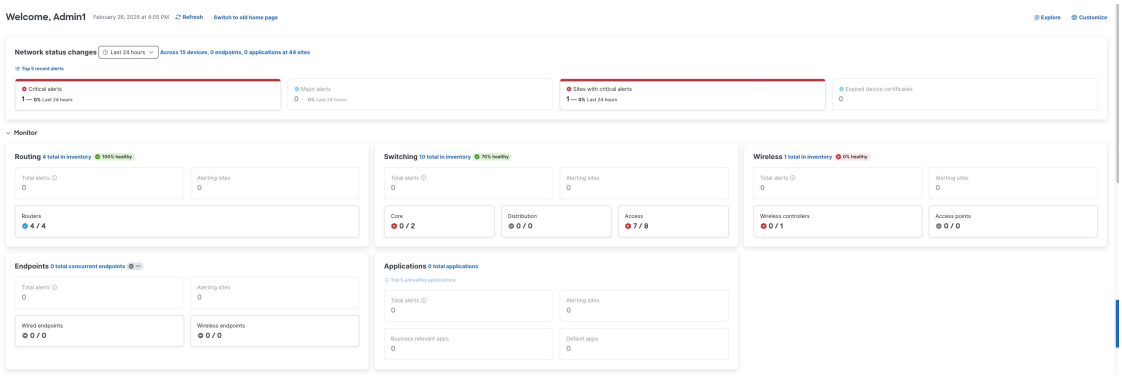
After you log in, you see the Catalyst Center home page. This page provides a granular summary view of your network, allowing you to quickly assess its overall performance, status, and health. The main menu, icons in the top-right portion of the window, and **Interactive Help** work the same as they did on the previous home page.

Different views of the home page

The home page can vary depending on different stages of Catalyst Center and what role is used to log in.

For example, the day-*n* view of the Catalyst Center home page displays when there are devices in inventory.

Figure 1: The day-n view of the Catalyst Center home page



Quick actions

You can:

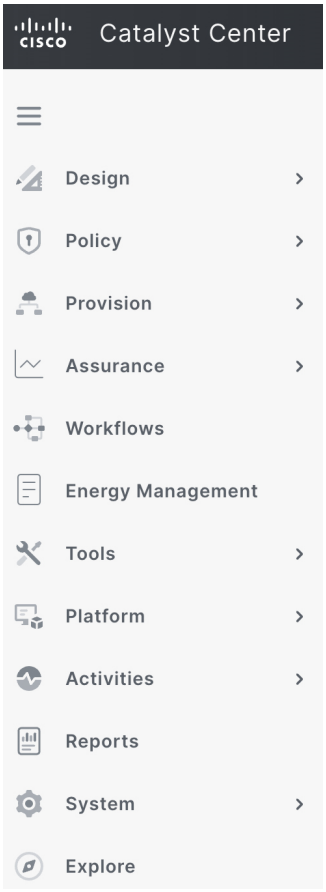
- Click **Refresh** at the top of the page to manually update the home page data.
- Click **Switch to old home page** at the top of the page to view the previous home page.

  At the top of the old home page, click **Switch to new home page** to return to the default home page.
- Click **Explore** in the top-right corner of the page to view the Catalyst Center journey map on the **Explore** page. For more information, see Catalyst Center journey map, on page 35.

Main menu

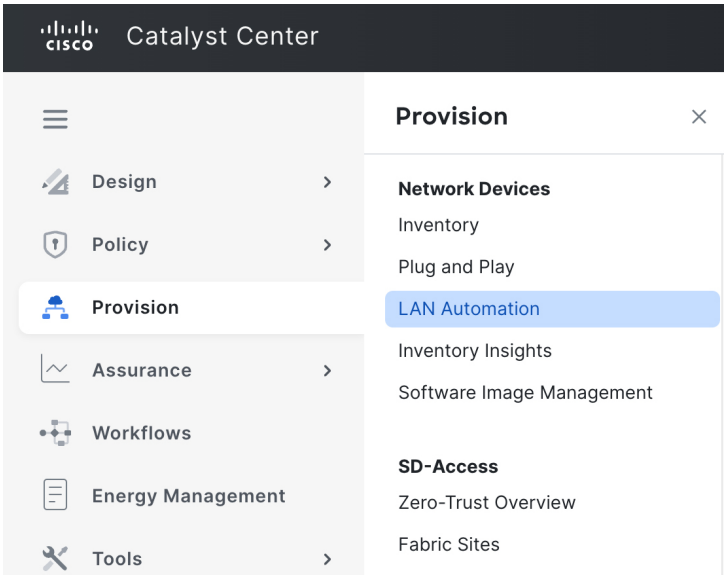
From the Catalyst Center main menu, you can access the many network management features that Catalyst Center provides.

Figure 2: Catalyst Center main menu



To open a particular Catalyst Center page, either click or hover your cursor over the appropriate menu option to view its submenu. Then click the link for the page that you want to open, such as the **LAN Automation** page.

Figure 3: Catalyst Center submenu



Some options (such as **Workflows**) don't have a submenu. You can open them directly from the main menu.

By default, Catalyst Center displays the main menu labels. To display or hide these labels, click the **Expand**/**Collapse** icon (☰).

Toolbar icons and help options

The top-right portion of the Catalyst Center window is the toolbar. You can click the icons in this toolbar to do common tasks. This table describes these icons.

Icon	Description
	Search: Search for devices, users, hosts, menus, and other items that are stored anywhere in the Catalyst Center database.
	Favorite: Add any window on Catalyst Center to your favorites to navigate to it easily and quickly. For more information, see Add a window to your favorites, on page 40.
	Help: View a list of help options. For more information, see Help menu options.
	Software Updates: See a list of available software updates. Click the **Go to Software Updates** link to view system and application updates.
	Notifications: View event notifications and set notification preferences. A red circle next to the notification icon shows that new notifications are available.

Help options

In the toolbar, click the help icon to view the help options. This table describes these options.

Option	Description
API Reference	Open the Catalyst Center platform API documentation in Cisco DevNet.
About	Displays the current Catalyst Center software version. • Click **Release Notes** to launch the release notes in a separate browser tab. • Click **Packages** to view the system and application package versions. • Click **Serial number** to view the serial number of the Catalyst Center appliance. • Click **Member ID** to view the member ID.
Developer Resources	Open Cisco DevNet, where you can access developer tools.
Contact Support	Open a support case with Cisco Technical Assistance Center (TAC).
Help	Open context-sensitive online help in a separate browser tab.
Cisco Support Assistant	Open a support case with Cisco Technical Assistance Center (TAC). • Click **Open support case** to submit a new support case. • Click **Cases list** to view the status of cases submitted. • Click **Record screen** to capture a recording of the issue for troubleshooting. • Click **Upload file** to upload your screen recording or other relevant file to a new or existing support case.
Remote Support Authorization	Grant remote access to a Cisco specialist to access Catalyst Center for troubleshooting your network. For more information, see View the remote support authorization dashboard, on page 36.
Cisco CX Cloud Success Tracks	Access the Cisco CX cloud success tracks website in a new window.
Keyboard Shortcuts	Display the keyboard shortcut names, shortcut keys, and shortcut key combinations for shortcut groups.
Make a Wish	Submit your comments and suggestions to the Catalyst Center product team.

Default sections on the home page

The home page is organized into these default sections:

- Network status changes
- Monitor
- Compliance and other notices

- Device advanced features

Each section has interactive and noninteractive elements. You can click an interactive element in a section, such as hyperlinked text or a card, to go to the relevant Catalyst Center page for more information or management tasks.

Network status changes

This section displays recent data for alerts and expired device certificates.

This table describes how you can filter and view the recent network status data in the **Network status changes** section.

If you want to...	Then...
filter the data in this section for a specific time range,	from the **Last <*time range*>** drop-down list, choose a time range option to view the network status changes for that time range. The data in this section is updated based on your time range selection.
view the devices with recent network status changes based on your time range selection,	click **Across <*number of*> devices, <*number of*> endpoints, <*number of*> applications at <*number of*> sites**. The **Provision** > **Inventory** page appears.
view the top five recent alerts,	click **Top 5 recent alerts**. The slide-in pane opens and lists the top five recent critical and major alerts, along with their priority, name, site, and severity.

This table describes the cards in the **Network status changes** section.

Note Understand these definitions for critical and major issues:

- P1: Critical issues that need immediate attention before they cause a wider impact on network operations.
- P2: Major issues that can potentially impact multiple devices or clients.

Card name	Description
Critical alerts	Displays the number of critical alerts. Click this card to view all open critical (P1) issues on the **Assurance** > **Issues and Events** dashboard. Refer to "View and Manage Issues" in the *Cisco Catalyst Assurance User Guide*.
Major alerts	Displays the number of major alerts. Click this card to view all open major (P2) issues on the **Assurance** > **Issues and Events** dashboard. Refer to "View and Manage Issues" in the *Cisco Catalyst Assurance User Guide*.

Card name	Description
Sites with critical alerts	Displays the number of sites with critical alerts. Click this card to view the sites impacted by critical (P1) issues on the **Assurance** > **Issues and Events** dashboard. Refer to "View and Manage Issues" in the *Cisco Catalyst Assurance User Guide*.
Expired device certificates	Displays the number of expired device certificates.

Monitor

This collapsible section displays network monitoring data for routing, switching, wireless, endpoints, applications, and Software-Defined Access (Cisco SD-Access).

This table describes the dashlets in the **Monitor** section.

Note If there are no routing, switching, or wireless devices in inventory, the system displays **Add devices** instead of **<*Number of*> total in inventory** in the relevant dashlet.

Dashlet name	Description
Routing	Displays the total number of alerts, alerting sites, and routers. Click **<*Number of*> total in inventory** to view all routers in inventory on the **Provision** > **Inventory** page. Refer to Manage Your Inventory, on page 77.
Switching	Displays the total number of alerts, alerting sites, and switches (core, distribution, and access). Click **<*Number of*> total in inventory** to view all switches in inventory on the **Provision** > **Inventory** page. Refer to Manage Your Inventory, on page 77.
Wireless	Displays the total number of alerts, alerting sites, wireless controllers, and access points (APs). Click **<*Number of*> total in inventory** to view all APs and wireless controllers in inventory on the **Provision** > **Inventory** page. Refer to Manage Your Inventory, on page 77.
Endpoints	Displays the total number of alerts, alerting sites, and wired and wireless endpoints. Click **<*Number of*> total concurrent endpoints** to go to the **Assurance** > **Health** dashboard for client health. Refer to "Monitor and Troubleshoot Client Health" in the *Cisco Catalyst Assurance User Guide*.

Dashlet name	Description
Applications	Displays the total number of alerts, alerting sites, and business-relevant and default applications. • Click **<*Number of*> total applications** to go to the **Assurance** > **Health** dashboard for application health. • Click **Top 5 unhealthy applications** to view a slide-in pane that lists the top five unhealthy applications affected by any critical and major alerts. Refer to "Monitor Application Health" in the *Cisco Catalyst Assurance User Guide*.
Software-Defined Access	**Note** This dashlet is visible only if the Cisco SD-Access package is installed. Displays the total number of alerts, fabric sites, Layer 3 virtual networks, and Cisco SD-Access transits. Click **<*Number of*> total fabric sites** to go to the **Assurance** > **Health** dashboard for Cisco SD-Access health. Refer to "Monitor and Troubleshoot SD-Access Health" in the *Cisco Catalyst Assurance User Guide*.

Compliance and other notices

This collapsible section displays notice data for software image management (SWIM), compliance, security, licensing, system, and recent activity.

This table describes the dashlets in the **Compliance and other notices** section.

Dashlet name	Description
Software Images	Displays the number of devices with high and critical advisories, devices without a standard image, and devices that failed image updates. Click **<*Number of*> total software images** to go to the **Provision** > **Software Image Management** page. Refer to Manage Software Images, on page 533.

Dashlet name	Description
Security	**Note** This dashlet is visible only if the Rogue and aWIPS package is installed. Displays the number of rogue threats, aWIPS threats, total unique rogue clients, critical advisories, and high advisories. • Click ***<Number of>*** **total advisories** to go to the **Tools** > **Security Advisories** page. Refer to Identify Network Security Advisories, on page 1349. • Click the number for rogue threats, aWIPS threats, or total unique rogue clients to go to the **Assurance** > **Rogue and aWIPs** dashboard. Refer to "Monitor the Rogue and aWIPS Dashboard" in the *Cisco Catalyst Center Rogue Management and aWIPS Application Quick Start Guide*.
Config Compliance	Displays the number of devices without network settings and devices with conflicting configurations. Click ***<Number of>*** **total of non compliant devices** to go to the **Provision** > **Inventory** page. On this page, the system has automatically filtered for all noncompliant devices. Refer to Compliance Audit for Network Devices, on page 561.
Recent Activities	Displays the number of • successful, in-progress, and failed activities • provisioning tasks in the last seven days • image upgrades in the last seven days, and • configuration compliance remediations in the last seven days. Click ***<Number of>*** **total activities in last 7 days** or the number of successful, in-progress, or failed activities to go to the **Activities** > **Tasks** page. On this page, the system has automatically filtered for all relevant activities from the last seven days. Refer to "View, edit, stop, and delete tasks" and "View and discard work items" in the *Cisco Catalyst Center Administrator Guide*.
Licenses	Displays the number of • devices that need registration • devices that are out of compliance, and • licenses that will expire in one month. Click ***<Number of>*** **total devices with licenses** or the number of devices needing registration to go to the **Tools** > **License Manager** page. Refer to "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Dashlet name	Description

System	This dashlet displays two types of data:
	• System:
	  • Displays the total number of services and services that are down. Click either of these numbers to go to the **System** > **System 360** page. Refer to "Use System 360" in the *Cisco Catalyst Center Administrator Guide*.
	  • Displays the cloud connectivity status, which indicates if the system is connected to the Cisco software catalog. Refer to "Manage Applications" in the *Cisco Catalyst Center Administrator Guide*.
	• Certificate expiring: Displays the number of trusted certificates, device certificates, and system certificates. Refer to "Security recommendations" in the *Cisco Catalyst Center Administrator Guide*.

Device advanced features

This collapsible section displays device data for network bugs, field notices, and end-of-life (EoX) alerts.

This table describes the dashlets in the **Device advanced features** section.

Dashlet name	Description
Network Bugs	Displays the number of network bugs with critical or high severity. Click **<*Number of*> total network bugs** to go to the **Tools** > **Network Bug Identifier** page. Refer to Identify Network Bugs, on page 1345.
Field Notices	Displays the number of hardware and software field notices that affect devices in your network. Click **<*Number of*> total field notices** to go to the **Tools** > **Field Notices** page. Refer to Identify Network Field Notices, on page 1367.
EoX Milestones	Displays the number of EoX alerts and the number of EoX alerts for the hardware, software, and module components of the devices in inventory. Click **<*Number of*> total EoX alerts** to go to the **Provision** > **Inventory** page. Refer to Display information about your inventory, on page 80.

Network and activity status icons

On the home page, you can view status icons in the sections to quickly assess various network metrics. This table describes each status icon.

Icon	Description	Example
	Healthy, successful, or connected	For example, when the Routing dashlet displays this status with a percentage, it indicates that the routers in inventory are healthy. When the Recent Activities dashlet displays this status, it indicates that a specific number of activities are successfully completed.
	Connected	For example, when the Critical Alerts dashlet displays this status, it indicates that there are no recent critical alerts.
	In progress	For example, when the Recent Activities dashlet displays this status, it indicates that a specific number of tasks are in progress.
	Unhealthy, failed, or out of compliance	For example, when the Wireless dashlet displays this icon with a percentage, it indicates that the wireless devices are not healthy. When the Software Images dashlet displays this icon, it indicates that a specific number of device families do not have a standard image applied to them.
	Status is not available	For example, when the Endpoints dashlet displays this status, it indicates that the status of endpoints in inventory is not available.

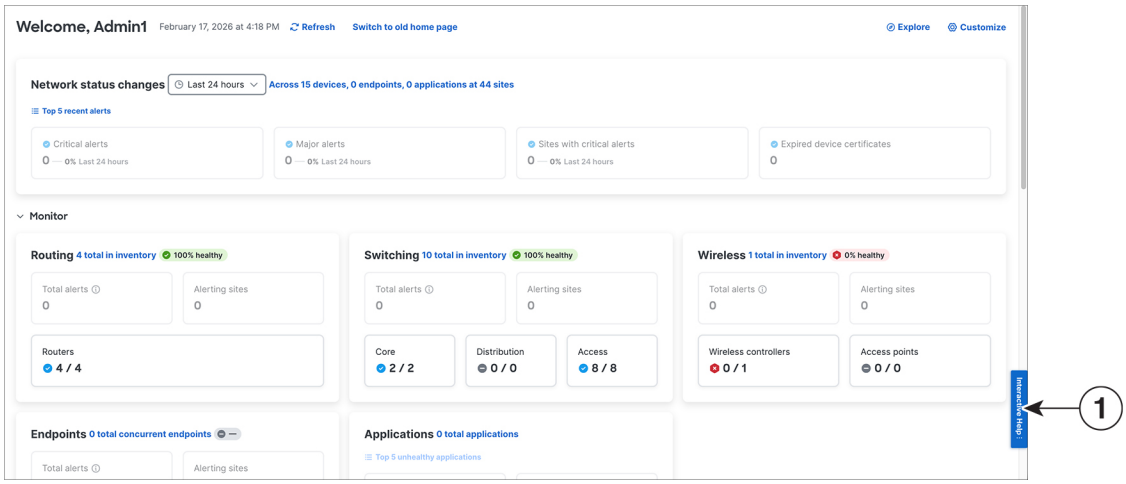
Interactive Help

Interactive Help contains walkthroughs for specific tasks in Catalyst Center. The walkthroughs provide onscreen guidance to help you complete the task.

You can open **Interactive Help** by using one of these methods:

- Click the Help icon and choose **Interactive Help**.
- Click the **Interactive Help** widget displayed by default in the bottom-right corner of the Catalyst Center window.

Figure 4: Interactive Help widget



This table describes the callout for Interactive Help widget figure.

1	**Interactive Help** widget

You can move the **Interactive Help** widget (callout 1) from the default location to other locations on the GUI window. Drag and drop the widget to the possible locations, which are indicated by green dotted-line rectangles.

You can move **Interactive Help** pop-ups by dragging their top border and dropping them in a new location on the GUI window. However, if the **Interactive Help** pop-up is associated with a specific menu option, you cannot move it.

Customize the home page

Use this procedure to customize the Catalyst Center home page.

Procedure

Step 1 On the home page, click **Customize** in the top-right corner.

Step 2 In the **Customize** slide-in pane, do these steps:

a) Customize the home page using any of these actions:

- Click **rename** next to a section name to rename it.
- Click the delete icon ( ) to delete a section.
- Click the toggle button next to a dashlet name to show or hide that dashlet on your home page.
- Drag and drop the drag-and-drop icon ( ) next to a section or dashlet name to reorganize your home page.
- From the **+ Add Section** drop-down list, choose **New Section** to add a new section on your home page. Then use the **+ Add Dashlet** drop-down list to add a dashlet to this new section.

b) After making your changes, click **Apply** to update the home page layout.

Action Required dialog box

If a known issue affects a cloud-tethered Catalyst Center cluster and the corrective action requires your approval, Catalyst Center displays an **Action Required** dialog box on the home page.

Review the information in the dialog box and select the required response. For more information, refer to Approve or decline a corrective action, on page 1471.

Reauthenticate Cisco.com and Smart Account credentials

Cisco has implemented a new authentication infrastructure. As a result, if you upgraded to Catalyst Center Release 2.3.7.9 or later, a message at the top of the home page indicates that the cisco.com and Smart Account

credentials that were configured previously have expired. Click the **Cisco.com Credentials** and **Smart Account** links to open the relevant Catalyst Center window and reauthenticate these credentials.

Related information

See "Configure Cisco credentials" and "Configure Smart Account" in the *Cisco Catalyst Center Administrator Guide*.

Catalyst Center journey map

The Catalyst Center journey map shows various capabilities provided by Catalyst Center and its use.

Procedure

Step 1 To launch the Catalyst Center journey map, do any one of these tasks:

- From the main menu, choose **Explore**.
- In the Catalyst Center home page, click **Explore**.

In the Catalyst Center journey map, the various features (capabilities) provided by Catalyst Center are grouped into tabs, including **AIOps**, **NetOps**, **DevOps**, and **SecOps**. Hover your cursor over the ⓘ icon to view details about each tab.

Step 2 Click the ◷ icon to view the journey map in a pie chart.

The pie chart shows the details of the chosen tab. A number next to a step (for example, ①) indicates the suggested order of the recommended steps within a segment for your journey map. You can do these actions in the pie chart:

- Hover your cursor over the features displayed in the pie chart to view a brief description about the feature and its status.
- If a feature is installed or in use, click the feature name in your journey map to view its configuration or settings page.
- To view the details about a segment, click the segment name in the pie chart. To return to the previous view containing all the segments, click the segment name again.

Step 3 Click the ☰ icon to view the journey map in a table format.

The table shows the details of the chosen tab. Hover your cursor over the feature name to view a brief description about the feature and its status.

Step 4 Check the **Completed** check box to view information about the completed and incomplete steps in the journey map.

- If you click **Completed**, the completed steps are highlighted with green borders.
- If you click **Incomplete**, the incomplete steps are highlighted with orange borders.

View the remote support authorization dashboard

Remote support authorization allows you to grant remote access to a Cisco specialist to access Catalyst Center and troubleshoot your network.

Note The Catalyst Center remote support authorization is supported only with RADKit version 1.2.1 and later.

Procedure

Step 1 From the top-right corner, click the help icon (?) and choose **Remote Support Authorization**.

In the **Remote Support Authorization** dashboard, the **SUMMARY** area shows the total, current, and past remote support authorizations. The Remote Support Cloud service connectivity status shows in the top-right corner as:

- A green check mark indicates that the remote support authorization is connected to the Remote Support Cloud service.
- An exclamation point indicates that the remote support authorization is not connected to the Remote Support Cloud service.

Step 2 In the **Create New Authorization** tab, click **Create a Remote Support Authorization** to create a new authorization. For more information, see Create a remote support authorization, on page 1415.

Step 3 Click the **Current Authorizations** tab to view the current remote support authorization tiles with various statuses, including:

- **All**: Displays all the scheduled and active remote support authorizations.
- **Scheduled**: Displays the scheduled remote support authorizations.
- **Active**: Displays the active remote support authorizations.

For troubleshooting purposes, the support authorization tile shows the schedule and duration of the Cisco specialist's access to Catalyst Center.

Step 4 To revoke an authorization, click **Revoke Authorization** in the respective support authorization tile.

Step 5 Click the **Past Authorizations** tab to view the past authorizations.

The **Past Authorizations** table shows the support authorization based on **Case Number**, **Date**, **Session Status**, **Cisco Specialist**, and **Log** and lists these statuses for past authorizations:

- **All**: Lists all the expired and revoked remote support authorizations.
- **Expired**: Lists all the expired remote support authorizations.
- **Revoked**: Lists all the revoked remote support authorizations.

Using the search bar, you can search for past authorizations by case number.

Step 6 To view the remote support authorization logs, click **View Logs** for the desired authorization.

The **Audit Logs** window is displayed. For more information, see "View Audit Logs" in the *Cisco Catalyst Center Administrator Guide*.

Use global search

Use the global search function to find items in these categories anywhere in Catalyst Center:

- **Activities**: Search for Catalyst Center menu items, workflows, and features by name.
- **Applications**: Search for them by name.
- **Application Groups**: Search for them by name.
- **Authentication template**: Search for them by name or type.
- **Devices**: Search for them by collection status, reachability status, location, or tag.
- **Fabric**: Search by fabric name.
- **Feature Templates**: Search for them by feature template name or parameter name.
- **Help**: Search for topics that include your search string.
- **Hosts and Endpoints**: Search for them by name, IP address, or MAC address.
- **IP Pools**: Search for them by name or IP address.
- **Network Devices**: Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.
- **Network Profiles**: Search by profile name.
- **Network Settings**
  - **Device Credentials**: Search by name.
  - **IP Address Pools**: Search for them by group name or pool CIDR.
  - **Service Provider Profiles**: Search for them by profile name, WAN provider, or model.
  - **Wireless Network Settings**: Search for them by wireless network settings name or parameter name.
- **Policy**: Search for them by name or description.
- **Sites**: Search for them by name.
- **Traffic copy**: Search for them by name and description.
- **Transits**: Search by transit name.
- **Users**: Search for the system settings and users by username. Case-insensitivity and substring search are not supported for usernames.
- **Workflows**: Search for them by task name or parameter name.
- Other items, as new versions of Catalyst Center are released.

To start a global search, click the search icon () in the top-right corner of any Catalyst Center window. Catalyst Center displays a global search window, with a search field where you can begin entering identifying information about an item.

You can enter all or part of the item's name, address, serial number, or other identifying information. The search field is case-insensitive and can contain any character or combination of characters.

As you begin entering your search string, Catalyst Center displays a list of possible search targets that match your entry. If more than one category of item matches your search string, Catalyst Center sorts them by category, with a maximum of five items in each category. The first item in the first category selects automatically, and summary information for that item is displays in the summary panel on the right.

You can scroll the list as needed, and click any of the suggested search targets to see information for that item in the summary panel. If there are more than five items in a category, click **View All** next to the category name. To return to the categorized list from the complete list of search targets, click **Go Back**.

As you add more characters to the search string, global Search automatically narrows the displayed list.

Catalyst Center allows you to search for a device using its entire IPv6 address or any abbreviated form of the IPv6 address.

For example, to search for *2001:0db8:85a3:0000:0000:8a2e:0370:7334*, you can use these search entries:

- **`2001:0db8:85a3:0000:0000:8a2e:0370:7334`** (using the full IPv6 address)
- **`2001:db8:85a3:0:0:8a2e:0:7334`** (truncating leading zeros)
- **`2001:db8:85a3::8a2e:0:7334`** (compressing consecutive zeros with a double colon)
- **`2001:db8:85a3`** (using a portion of the IPv6 address)

Catalyst Center allows you to search for an IPv6 address by using the double colon in the IPv6 address with prefix, postfix, or any combination.

For example, to search for *2001:db8:85a3::8a2e:0:7334*, you can use these search entries:

- **`::`** (using double colon alone)
- **`85a3::8a2e`** (using prefix and postfix with double colon)
- **`85a3::`** (using prefix with double colon)
- **`::8a2e`** (using postfix with double colon)

You can search for devices in Catalyst Center by entering their MAC addresses in any format (with a hyphen or colon).

When users with scope-based access permissions search for network devices by device name or client ID or IP address, no device details are displayed. However, searching by MAC address shows device data limited to the device or client 360 cross-launch link.

Global search can display five results per category at a time.

The search occurs on data that is synchronized every 10 minutes. Therefore, after a change occurs, the search results reflect the change after up to 10 minutes.

Set the clock format to 12 hours or 24 hours

You can set a 12-hour or 24-hour display format for time across the GUI.

Procedure

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **Display Settings**.

Step 2 In the **Set Clock Format** area, click **12 hours** or **24 hours**.

Step 3 Click **Save**.

Apply light or dark appearance in Catalyst Center

You can view Catalyst Center in light (default) or dark appearance.

Procedure

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **Display Settings**.

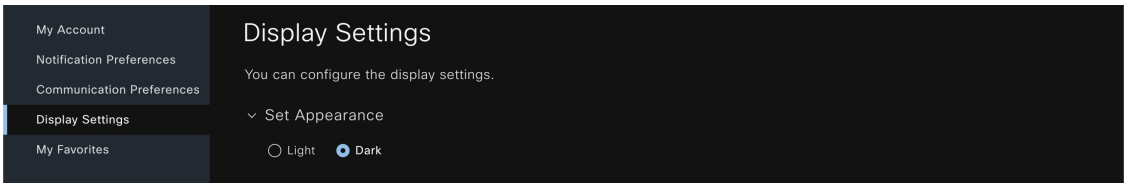
Step 2 In the **Set Appearance** area, click **Light** or **Dark** to view Catalyst Center in light appearance or dark appearance.

Step 3 Click **Save**.

Catalyst Center caches the appearance you choose in the browser storage. Therefore, in these scenarios where the browser cache that stores the appearance is not available, the Catalyst Center GUI displays in light appearance for several seconds:

- You log in to Catalyst Center from a different browser.
- In a three-node cluster, you log in to the second or third Catalyst Center node for the first time after dark appearance is applied in a primary node.

When dark appearance is enabled, the Catalyst Center GUI displays like this example:



Enable localization

You can view the Catalyst Center GUI windows in English (the default), Chinese, Japanese, or Korean.

To change the default language:

Procedure

Step 1 In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

- From Google Chrome:
  a. Click the icon in the top-right corner, and then select **Settings**.
  b. Click **Languages**.
  c. Click **Add languages**.
  d. In the **Add languages** dialog box, select **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
- From Mozilla Firefox:
  a. Click the icon in the top-right corner, and then select **Settings**.
  b. From the **Language and Appearance** > **Language** area, click **Choose**.
  c. From the **Select a language to add** drop-down list, select **Chinese**, **Japanese**, or **Korean**.
  d. Click **OK**.

Step 2 Log in to Catalyst Center.

The GUI shows in the selected language.

Add a window to your favorites

You can add any window on Catalyst Center to your favorites (the list of your favorited windows). With your favorites, you can navigate to favorited windows more easily and quickly.

You can also add different views of the same window to your favorites if the view has a unique URL. For example, on the **Tasks** window, you can add this window to your favorites when it's filtering tasks or work items with the **Success** status and, separately, when it's filtering tasks or work items with the Last Updated **24 hours** status.

Procedure

Step 1 Navigate to the window that you want to add to your favorites.

Step 2 On the window, in the top-right corner, click the star icon ( ) to add the window to your favorites.

Step 3 On the **This window is favorited** dialog box, in the **Name** field, you can either:

a) Keep the autopopulated name as the title of your favorited window.
b) Delete the autopopulated name and type a new name.

Step 4 (Optional) To view the list of your favorited windows, click **View my favorites**.

The **My Favorites** slide-in pane displays all your favorited windows.

Tip To quickly display the **My Favorites** slide-in pane from any window on Catalyst Center, use the keyboard shortcut **q** + **f**.

Step 5 Click **Done** to save any edits to the favorited window name and to close the dialog box.

Step 6 (Optional) To remove a window from your favorites, you can either remove it from the **This window is favorited** dialog box or the **Favorites Preferences** window.

a) Navigate to the favorited window that you want to remove, and then click the star icon ( ). In the **This window is favorited** dialog box, click **Remove**.
b) To remove a window from your favorites, see Manage your favorites, on page 41.

Manage your favorites

You can manage your favorited windows on the **Favorites Preferences** window. For information about adding a window to My Favorites, see Add a window to your favorites, on page 40.

Procedure

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **Favorites Preferences**.

The **Favorites Preferences** window displays the list of your favorited windows.

Step 2 (Optional) To remove a favorited window:

a) Locate the favorited window that you want to remove from the list.
b) Click the star icon ( ) next to the favorited window to remove it from the list.

Step 3 (Optional) To go to a favorited window:

a) Locate the favorited window that you want to go to.
b) Under the favorited window, click its hyperlinked pathway.

Subscribe to Catalyst Center Insights

You can subscribe to *Catalyst Center Insights*, which contains product announcements, network highlights, information about your network performance, and more. The Catalyst Center Insights publication is sent in PDF format to the email address that you specify.

Note If your Catalyst Center appliance is deployed in a secure, air-gapped network, certain metrics are omitted from Catalyst Center Insights. To view the complete Catalyst Center Insights, you must have internet and telemetry connectivity, which aren't available in air-gapped environments.

Before you begin

- Under **System** > **Settings** > **Integration Settings**, enter your callback URL hostname or IP address. For more information, see "Configure Integration Settings" in the *Cisco Catalyst Center Administrator Guide*.
- Under **System** > **Settings** > **External Services** > **Destinations** > **Email**, configure the SMTP servers that you will use to receive the publication.

Procedure

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **Communication Preferences**.

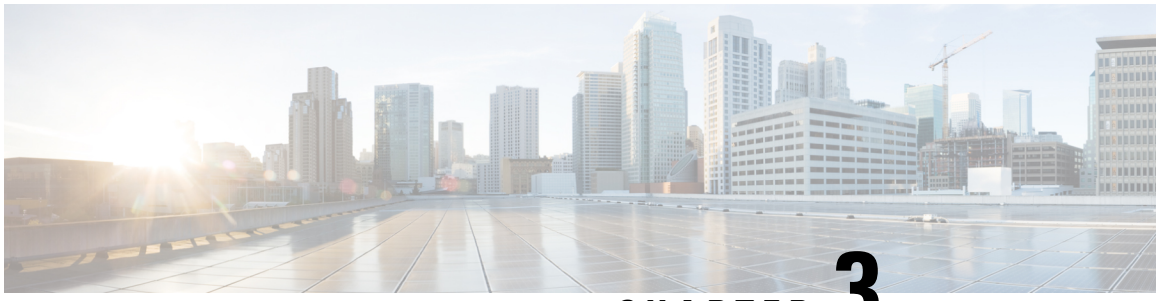
Step 2 Click the **Subscription Off** toggle button to **Subscription On**.

Step 3 Enter the email address where you want to receive Catalyst Center Insights, and click **Save**.

Insights are archived for up to one year. You can read past publications by choosing **Actions** > **Download PDF** for the desired date range.

Step 4 (Optional) To change the email address, click the pencil icon.

Step 5 (Optional) To unsubscribe from Catalyst Center Insights, click the **Subscription On** toggle button to **Subscription Off**.



CHAPTER 3

Configure Telemetry

- About telemetry settings, on page 43
- Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 43
- Criteria for enabling application telemetry on devices, on page 45
- Provision application telemetry settings, on page 47
- Enable application telemetry for wireless controllers, on page 47
- Update application telemetry to use a new cluster virtual IP address, on page 49
- Update device configuration using telemetry, on page 50

About telemetry settings

Catalyst Center allows you to configure and update global telemetry parameters on devices, such as syslog, SNMP traps, and wired client data collection. You can enable or disable application telemetry. Enabling application telemetry lets you configure Netflow collector settings on devices to monitor and assess their health.

Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry

With Catalyst Center, you can configure global network settings when devices are assigned to a specific site. Telemetry polls network devices and collects telemetry data according to the settings in the SNMP server, syslog server, NetFlow Collector, or wired client.

Before you begin

Create a site and assign a device to the site. See Create, edit, and delete a site, on page 240.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Telemetry**.

Step 2 In the **SNMP Traps** area, do one of these tasks:

- Check the **Use Catalyst Center as SNMP trap server** check box.
- Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server. The selected server collects SNMP traps and messages from the network devices.

Step 3 In the **Syslogs** area, do one of these tasks:

- Check the **Use Catalyst Center as syslog server** check box.
- Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

Step 4 In the **Application Visibility** area, check the **Enable by default on wired access devices** check box to enable Application Telemetry and Controller-Based Application Recognition (CBAR) by default upon the network device site assignment.

Do one of these tasks:

- Click the **Use Catalyst Center as NetFlow collector** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.
- Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.

Note Catalyst Center must be configured as a destination in Cisco Telemetry Broker to receive NetFlow records. If Catalyst Center is not configured as a destination, the Application Experience does not work.

Step 5 In the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button to turn on IP Device Tracking (IPDT) on the access devices of the site.

If you don't want to enable IPDT for the site, click the **Disable Catalyst Center Wired Endpoint Data Collection At This Site** radio button (the default).

After enabling IPDT, clients connected to access ports are visible in Catalyst Center. Clients connected to trunk ports and port channels aren’t visible in Catalyst Center.

Note You must enable IPDT to preview the CLI configuration. When provisioning a device, you can preview the CLI configuration before deploying it on the device.

For the Cisco Catalyst 9410R Switch running software version 17.5.1 or later, ports ending with 4/0/48 are intentionally skipped during IPDT configuration.

Step 6 In the **Wireless Controller, Access Point and Wireless Clients Health** area, check the **Enable Wireless Telemetry** check box to monitor the health of the wireless controllers, APs, and wireless clients in your network.

During the Device Controllability workflow, enabling Wireless Telemetry activates telemetry data collection and provisions telemetry commands to wireless configurations. When you disable this feature, telemetry setup stops, and monitoring capabilities are lost. For more information, see Device controllability in *Cisco Catalyst Center Administrator Guide*.

Step 7 Click **Save**.

Criteria for enabling application telemetry on devices

Catalyst Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Note

- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.
- If you want to switch over from the automatic selection algorithm to the tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.
- Tagging-based algorithm applies to both greenfield and brownfield deployments.

This table provides the criteria for selecting interfaces and WLANs using both the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms.

Platform	Conventional tagging-based algorithm	Automatic selection algorithm

Router	• Interface description has the **lan** keyword.[1], [2]
	• Interface has an IP address other than the management IP address.
		• Interface has an IP address other than the management IP address.
		• Interface is not any of these types:
		  • WAN
		  Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.
		  In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.
		  Route rules can be dynamically learned. In this context, the **show ip route** command does not show a route to a public IP address that goes through this interface.
		  • Loopback.
		  • Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.

Platform	Conventional tagging-based algorithm	Automatic selection algorithm

Switch	• Interface description has the **lan** keyword.[1, 2]
	• Switch port is configured as an access port.
	• Switch port is configured with the **switch-mode access** command.
		• Interface is a physical interface.
		• Access port does not have neighbors.
		• Interface is not any of these types:
		  • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0
		  • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async
		  • VSL interface.

Cisco AireOS Controller	WLAN profile name is tagged with the **lan** keyword.[1, 2]	If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, Wireless Service Assurance (WSA) processing is enabled. If all the SSIDs are in Local mode, NetFlow is enabled.
Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS 16.12.1 and later.	WLAN profile name is tagged with the **lan** keyword.[1, 2]	If the SSIDs are mixed—that is, central switching, Flex mode, and Fabric mode—the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs use central switching, the Optimized APM record is configured. For Cisco Catalyst 9800 Series Wireless Controllers with IOS 17.10 and later, Catalyst Center pushes the APM profile, not the AVC basic profile, for flex and fabric SSIDs.
	Note NetFlow configurations are pushed to the policy profile with the "lan" keyword, not directly to the WLAN profile. In brownfield deployments, the workaround is to create a new policy profile with the "lan" keyword, delete the existing policy profile, and associate the new one with the existing WLAN profile. Renaming the policy profile directly is not supported.	
Catalyst Center Traffic Telemetry Appliance with Optimized APM profile and IOS 17.3 and later.	• Interface description has the **lan** keyword.[1, 2] • Interface is a physical interface.	• Interface is a physical interface. • Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

[1] The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.
[2] Resynchronize the network device to read the **lan** keyword.

For example, to use the conventional tagging-based algorithm to enable application telemetry:

- the WLAN profile name *test-lan* on this Cisco Catalyst 9800 Series Wireless Controller includes the **lan** keyword

```
WLAN Profile Name               SSID                      VLAN Status
-------------------------------------------------------------------------------
1    test-lan                   test1-ssid                137   UP
```

- the interface description *wired-lan* on this switch includes the **lan** keyword

```
interface GigabitEthernet1/0/1
description wired-lan
```

Provision application telemetry settings

You can configure NetFlow application telemetry settings on the device.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane and select the site, building, or floor.

Step 2 Select the devices that you want to provision.

Step 3 From the **Actions** drop-down list, select **Telemetry** and do one of these steps:

Note The **Enable Application Telemetry** and **Disable Application Telemetry** options are enabled only when the device supports application telemetry from Catalyst Center.

a) **Enable Application Telemetry**: To configure NetFlow application telemetry for the selected devices.
b) **Disable Application Telemetry**: To remove the NetFlow application telemetry configuration from the chosen devices.

Step 4 Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the **Application Telemetry** column in the default column setting, click the ellipsis icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

Enable application telemetry for wireless controllers

You can enable application telemetry for new and existing devices.

Note You can also enable Application Telemetry from the **Application Visibility** window. For more information, see Enable Application Telemetry, on page 1120.

Before you begin

To enable application telemetry, devices must have the Advantage license.

Note Before enabling application telemetry in Catalyst Center, manually delete any existing flow monitors from the **Configuration** > **Services** > **Application Visibility** > **Flow Monitors** section in the Cisco Catalyst 9800 Series Wireless Controller interface.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

Step 2 To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor.

Step 3 In the **Inventory** window, select the device. You can select multiple devices at a time.

Step 4 From the **Action** drop-down list, choose **Telemetry** > **Enable Application Telemetry**.

Step 5 In the **Enable Telemetry** slide-in pane, complete these settings:

a) AP mode: Check the **Flex/Fabric** or **Local** check box. You can also select both options.

b) To enable telemetry for guest SSIDs, check the **Include Guest SSID** check box.

Note If an SSID name contains the **guest** keyword, check the **Include Guest SSID** check box to enable telemetry, even if the SSID belongs to an enterprise wireless network.

c) **Telemetry Source**:

- Embedded Wireless Controllers - NetFlow
- AireOS wireless controller (Local mode) - NetFlow
- AireOS wireless controller (Flex/Fabric mode) - Wireless Service Assurance (WSA)

d) To apply the same settings for all wireless controllers, check **Apply this selection to all wireless controllers**.

e) Click **Next**.

f) Select the **Generate Configure Preview** radio button, then click **Preview**.

In the **Enable Application Telemetry Task** window, Catalyst Center displays a side-by-side comparison of the running configuration and the planned configuration for the first listed device.

In the **Enable Application Telemetry Task** window, do these tasks:

- Review the device configurations and then, when you're ready, click **Deploy**.
- Select the **Now** or **Later** scheduling option and click **Deploy**.

Note The **Application Telemetry** column shows the application telemetry deployment status.

If the application telemetry deployment fails for a device, click the link under **Application Telemetry Deployment Status** column to view the failure reason.

Update application telemetry to use a new cluster virtual IP address

If you are using the Catalyst Center application telemetry to monitor device data, and you need to change the Catalyst Center enterprise virtual IP address (VIP), complete these steps to change the VIP and to ensure that node telemetry data is sent to the new VIP.

Before you begin

- Determine the version of Catalyst Center that you are using. You can check for the version by logging in to the Catalyst Center GUI and using the **About** option to view the Catalyst Center version number.
- Obtain SSH client software.
- Identify the VIP address that was configured for the 10-GB interface facing the enterprise network on the Catalyst Center primary node. Log in to the appliance using this address, on port 2222. To identify this port, see the rear-panel figure in the "Front and Rear Panels" section in the *Cisco Catalyst Center Installation Guide*.
- Get the Linux username (**`maglev`**) and password configured on the primary node.
- Identify the cluster VIP that you want to assign. The cluster VIP must conform to the requirements explained in the "Required IP Addresses and Subnets" section in the *Cisco Catalyst Center Installation Guide*.

Procedure

Step 1 Use the appliance Configuration wizard to change the cluster VIP:

a) Using an SSH client, log in to the VIP address that was configured for the 10-GB interface facing the enterprise network on the Catalyst Center primary node. Be sure to log in on port 2222.

b) When prompted, enter the Linux username and password.

c) Enter this command to access the Configuration wizard on the primary node:

```
$ sudo maglev-config update
```

If you are prompted for the Linux password, enter it again.

d) Click **[Next]** until the screen prompting you for the cluster virtual IP appears. Enter the new cluster VIP, then click **[Next]** to proceed through the remaining screens of the wizard.

You must configure one virtual IP per configured interface. We recommend that you enter the **sudo maglev-config update** command so that the wizard prompts you to provide one VIP per configured interface.

When you reach the final screen, a message appears, stating that the wizard is ready to apply your changes.

e) Click **[proceed]** to apply the cluster VIP change.

At the end of the configuration process, a success message appears and the SSH prompt reappears.

Step 2 Restart the necessary Catalyst Center services by entering this series of commands at the SSH prompt:

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```

Step 3 Wait until all services restart. You can monitor the progress of the restarts by entering this command, substituting service names as needed for the release train appropriate for your Catalyst Center version.

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e
wirelesscollector
```

When all the necessary services are running, you see command output similar to this output, with a Running status for each service that has restarted successfully:

```
assurance-backend  wirelesscollector-123-bc99s  1/1   Running   0   25d   <IP>   <IP>
ndp   collector-netflow-456-lxvlx   1/1   Running   0   1d   <IP>   <IP>
ndp   collector-syslog-789-r0rr1    1/1   Running   0   25d   <IP>   <IP>
ndp   collector-trap-101112-3ppllm  1/1   Running   0   25d   <IP>   <IP>
```

Step 4 Access the Catalyst Center GUI and **Enable Application Telemetry** to all nodes:

a) From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

b) Select all the sites and devices that you want to monitor.

c) From the **Actions** drop-down list, choose **Telemetry** > **Enable Application Telemetry**.

d) Wait until the sites and devices show that telemetry is enabled.

Update device configuration using telemetry

Use this procedure to push configuration changes, including syslog, SNMP traps, NetFlow collectors, and wired client data collection changes, to a device. This applies regardless of whether device controllability is enabled or disabled.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the **Global** site in the left pane and choose the area, building, or floor.

Step 2 Choose the devices on which you want to update the configuration changes.

Step 3 From the **Actions** drop-down list, choose **Telemetry** > **Update Telemetry Settings**.

The **Update Telemetry Settings** slide-in pane opens.

Step 4 (Optional) Check the **Force Configuration Push** check box to send the configuration changes to the device.

If there is no change in the configuration settings, the existing configuration is pushed again to the device. The configuration repush does not occur consistently across all settings. This option triggers the Device Controllability workflow. This behavior depends on each configuration under device controllability.

For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.

Step 5 Click **Next**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.



Note During configuration preview, the PKCS12 certificate isn't generated as the certificate must be used within 15 minutes. The **Preview Configuration** window displays only the relevant configuration commands. When you deploy the configuration after previewing it, the PKCS12 certificate is generated and pushed to the device.

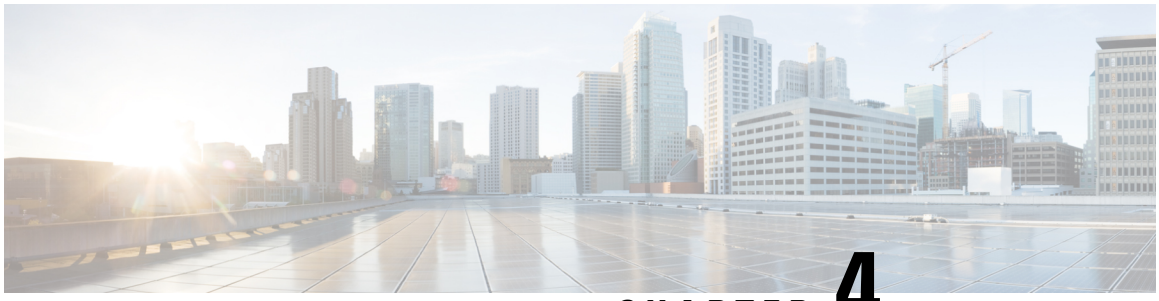
Step 7 On the **Tasks** window, monitor the task deployment.



PART II

Discover and Manage Network Inventory and Topology

- Discover Your Network, on page 55
- Manage Your Inventory, on page 77
- Display Your Network Topology, on page 219



CHAPTER 4

Discover Your Network

- Discovery overview, on page 55
- Discovery dashboard, on page 56
- Discovery prerequisites, on page 56
- Discovery credentials, on page 57
- Preferred management IP addresses, on page 63
- Discovery configuration guidelines and limitations, on page 64
- Do Discovery, on page 65
- Manage Discovery jobs, on page 73

Discovery overview

A Discovery method is a network discovery technique that

- scans devices in your network using multiple protocols or IP ranges,
- sends the list of discovered devices to inventory for management, and
- coordinates with Device Controllability to automatically configure network settings on devices when those settings are missing.

There are four ways to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. You can include up to 4096 devices in the range.
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.
- Use Classless Inter-Domain Routing (CIDR) and provide a seed IP address.

When you configure the Discovery criteria, you can use settings to reduce the time needed to discover devices:

- **CDP Level** and **LLDP Level**: If you use CDP or LLDP as the Discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. If you need to discover fewer devices, set the level to a lower value.
- **Prefix Length**: If you use **CIDR** as a discovery method, you can set the prefix length value, which ranges from 20 to 30. The default value is 30.

- **Subnet Filters**: If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.
- **Preferred Management IP**: Whether you use CDP, LLDP, CIDR, or an IP address range, you can specify whether you want Catalyst Center to add any of the device's IP addresses or only the device loopback address.



Note For Cisco SD-Access Fabric and Cisco Catalyst Assurance, specify the device loopback address.

Regardless of the method you use, you must be able to reach the device from Catalyst Center and configure specific credentials and protocols in Catalyst Center to discover your devices. These credentials can be configured and saved in the **Design** > **Network Settings** > **Device Credentials** window or on a per job basis in the **Discovery** window.



Note If a device uses a first hop resolution protocol, such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device can be discovered and added to the inventory along with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that Catalyst Center retrieves for analysis.

Discovery dashboard

From the main menu, choose **Tools** > **Discovery** to view the **Discovery dashboard**. The **Discovery dashboard** shows the inventory overview, latest discovery, discovery type, discovery status, and recent discoveries.

You can search for a device using the **Search** field. You can also use the **Status** and **Type** drop-down lists to filter and view the device details. Click **Reset all** to clear the filter.

Click **Export** to export the discovery details as a CSV file.

Click **View scheduled discoveries** to monitor and manage all the scheduled network operations.

Click **Add discovery** to discover devices using different parameters. For more information, see Discovery credentials, on page 57.

Discovery prerequisites

Before you run Discovery, complete these minimum prerequisites:

- View the *Cisco Catalyst Center Compatibility Matrix* to understand which devices will be discovered by Catalyst Center.
- Understand that the preferred network latency between Catalyst Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)

- Ensure that at least one SNMP credential is configured on your devices for use by Catalyst Center. At a minimum, this configuration can be an SNMPv2C read credential. For more information, see Discovery credentials, on page 57.
- To allow Catalyst Center to discover and manage devices, configure SSH credentials on them. Catalyst Center discovers and adds a device to its inventory if at least one of these criteria is met:
  - The account that is being used by Catalyst Center to SSH into your devices has privileged EXEC mode (level 15).
  - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see Discovery configuration guidelines and limitations, on page 64.
- In a dual-stack IPv4/IPv6 environment, note these points:
  - During a single discovery session, if a device is reachable via both IPv4 and IPv6, Catalyst Center retains only the first address family detected. To prevent duplicate device entries, Catalyst Center ignores the secondary address family.
  - For site-based, role-based access control (SRBAC), discovery is restricted by site access groups. A device already discovered under one site access group cannot be rediscovered or managed under a different site access group.
  - When the loopback option is enabled, the system defaults to IPv6. If an IPv6 loopback is unavailable, the system automatically falls back to IPv4.
  - Catalyst Center supports cross-family neighbor discovery. Discovery sessions seeded with IPv4 can identify IPv6 neighbors, and sessions seeded with IPv6 can identify IPv4 neighbors via CDP or LLDP.

Discovery credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, HTTP, HTTPS, and NETCONF configuration values for the devices that you want to discover. You must specify the credentials based on the types of devices you are trying to discover:

- Network devices: CLI and SNMP credentials.



Note For NETCONF-enabled devices such as embedded wireless controllers, you must specify SSH credentials with admin privilege and select the NETCONF port.

- Compute devices (NFVIS): CLI, SNMP, HTTP, and HTTPS credentials.

Because the various devices in a network can have different sets of credentials, you can configure multiple sets of credentials in Catalyst Center. The discovery process iterates through all sets of credentials that are configured for the Discovery job until it finds a set that works for the device.

If you use the same credential values for the majority of devices in your network, you can configure and save them to reuse in multiple Discovery jobs. To discover devices with unique credentials, you can add job-specific Discovery credentials when you run Discovery jobs. You can configure up to 10 global credentials for each

credential type and define any five of them. If you need to define a job-specific credential, you can define five global credentials and one job-specific credential for each credential type.

To define credentials for a Discovery, click the menu icon and choose **Tools** > **Discovery** > **Add Discovery**. To continue, use these procedures and discovery credential information:

- Discover your network using CDP, on page 66
- Discover your network using an IP address range or CIDR, on page 68
- Discover your network using LLDP, on page 70

Table 4: CLI credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials. If authentication fails for CLI, Catalyst Center retries the authentication process for 300 seconds (5 minutes).
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Table 5: SNMPv2c credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Field	Description
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Table 6: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Select one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Select one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Select one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.

Table 7: SNMP properties

Field	Description
Retries	Number of times Catalyst Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

Table 8: HTTP and HTTPS credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Field	Description
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Table 9: NETCONF setting

Field	Description
Port	Port on the device. You can use one of these ports: • Port 830 (default). • Any other port that is available on the device. • A custom port that Catalyst Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.) If authentication fails for NETCONF, Catalyst Center retries the authentication process for 300 seconds (5 minutes).

Discovery credentials and Cisco ISE

If you are using Cisco ISE as an authentication server, the Discovery feature authenticates devices using Cisco ISE as part of the discovery process. To ensure that your devices are discovered properly, use these guidelines:

- Do not use Discovery credentials that have fewer than 4 alphanumeric characters. Cisco ISE requires at least 4 alphanumeric characters for both username and password. If the device credentials have fewer

than 4 characters, Catalyst Center cannot collect the device inventory data. The device goes into a partial collection state.

- Do not use credentials that have the same username, but different passwords, such as cisco with cisco123 and cisco with pw123. While Catalyst Center allows the discovery of devices with the same username but different passwords, Cisco ISE does not allow discovery with duplicate usernames. If a duplicate username is used, Catalyst Center cannot authenticate the device and collect its inventory data, and the device will go into a partial collection state.

For information on how to define Cisco ISE as a AAA server, see Add Cisco ISE or other AAA servers, on page 319.

Guidelines and limitations for Discovery credentials

Here are the guidelines and limitations for the Catalyst Center Discovery credentials:

- To change the device credentials used in a Discovery job, edit the job and deselect the credentials you no longer want to use. Next, add the new credentials and start discovery. For more information, see Change credentials in a Discovery job, on page 73.
- If you change a device credential after successfully discovering the device, subsequent polling cycles for that device fail. To correct this situation, use one of these options:
  - Use the Discovery tool to:
    - Run a new Discovery job with job-specific credentials that match the device's new credential.
    - Edit the existing Discovery job and rerun the Discovery job.
  - Use the Design tool to:
    - Create a new global credential and run a new Discovery job using the correct global credential.
    - Edit an existing global credential and use Copy and Edit to recreate the Discovery job. Alternatively, create a new Discovery job.
- If an ongoing Discovery polling cycle fails because of a device authentication failure, you can correct the situation using one of these options:
  - Use the Discovery tool to:
    - Stop or delete the current Discovery job. Run a new Discovery job with job-specific credentials that match the device credential.
    - Stop or delete the current Discovery job. Edit the existing job. Rerun the Discovery job.
  - Use the Design tool to:
    - Create a new global credential and run a new Discovery job using the correct global credential.
    - Edit an existing global credential and use Copy and Edit to recreate the Discovery job. Alternately, create a new Discovery job.

- Deleting a global credential does not affect previously discovered devices. These devices do not show authentication failure. However, the next Discovery job that tries to use the deleted credential will fail. The Discovery job will fail *before* it tries to contact any devices.

Discovery credentials example

The devices that form a typical network can have widely varying Discovery requirements. Catalyst Center lets you create multiple Discovery jobs to support these varying requirements. For example, assume that a network has 200 devices that form a Cisco Discovery Protocol (CDP) neighborhood. In this network, 190 devices share a global credential (Credential 0) and the remaining devices each have their own unique credential (Credential-1 through Credential-10).

For FIPS mode deployment, the discovery password must contain at least 8 characters.

To discover all the devices in this network using Catalyst Center, do this procedure:

Procedure

Step 1 Configure the CLI global credentials as Credential-0.

Step 2 Configure the SNMP (v2c or v3) global credentials.

Step 3 Run a Discovery job using one of the 190 device IP addresses (190 devices that share the global credentials) and the global Credential-0.

Step 4 Run 10 separate Discovery jobs for each of the remaining 10 devices using the appropriate job-specific credentials, such as Credential-1, Credential-2, Credential-3, and so on.

Step 5 Review the results in the **Inventory** window.

Preferred management IP addresses

When Catalyst Center discovers a device, it uses one of the device IP addresses as the preferred management IP address. The IP address can be that of a built-in management interface of the device, another physical interface, or a logical interface such as Loopback0. You can configure Catalyst Center to use the device loopback IP address as the preferred management IP address, provided the IP address is reachable from Catalyst Center.

When you select **Use Loopback IP** as the preferred management IP address, Catalyst Center determines the preferred management IP address as detailed in this table:

Table 10: Preferred management IP address determination criteria

If	Then
If the device has one loopback interface	Catalyst Center uses that loopback interface IP address.
If the device has multiple loopback interfaces	Catalyst Center uses the loopback interface with the highest IP address.

If	Then
If there is no loopback interface	Catalyst Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.) The system also uses the loopback interface with the highest IP address.
If there are no Ethernet interfaces	Catalyst Center uses the serial interface with the highest IP address.

After a device is discovered, you can update the management IP address from the **Inventory** window. For more information, see Update a device management IP address, on page 181.

Discovery configuration guidelines and limitations

This section describes the limitations and guidelines of device discovery.

- These are the guidelines and limitations for Catalyst Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:
  - Configure the CLI username and password with privileged EXEC mode (level 15). These credentials are the same CLI username and password that you configure in Catalyst Center for the Discovery function. Catalyst Center requires the highest access level to the device.
  - Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
  - Don’t change the default login method for a device's console port and the VTY lines. If a device is already configured with a AAA (TACACS) login, make sure that the CLI credential defined in the Catalyst Center is the same as the TACACS credential defined in the TACACS server.
- These are the guidelines and limitations for Catalyst Center to discover your wireless controllers and APs:
  - Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows won’t display any data.
  - After the wireless controllers are discovered, Catalyst Center displays the list of associated APs in the inventory. The listed APs are connected to the wireless controller either during the discovery or through inventory sync.

Note For any new APs that join the wireless controller after the inventory sync:

- If the wireless controller isn't assigned to a site or provisioned in Catalyst Center, you must do a manual resync.
- If the wireless controller is assigned to a site, when a new AP joins the wireless controller, an SNMP trap is triggered. Using this SNMP trap, Catalyst Center discovers the newly joined AP. A manual resync isn't necessary.
- If the wireless controller is assigned to a site, Device Controllability must be enabled. If Device Controllability is disabled during the site assignment and later enabled, you must manually sync new APs.

- Third-party devices can’t be discovered with the Catalyst Center discovery feature. You must add the third-party devices manually to your network. For more information, see Add a third-party device, on page 151.

Do Discovery

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, CIDR, or an IP address range.

Your devices must have the required device configurations, as described in Discovery prerequisites, on page 56.

- For IP address range discovery, the system includes only ping-reachable devices in the list of discovered devices. The system does not include devices that cannot be reached by ping.
- For CDP-, CIDR-, and LLDP-based discovery, these protocols respond to ping-unreachable IPs as well, so ping-unreachable devices are included in the list of discovered devices.
- For CDP-, CIDR- and LLDP-based discovery, configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)
- The Discovery function requires the correct SNMP read-only community string. If you do not provide an SNMP read-only community string, the Discovery function attempts to use the default read-only community string, public.
- During discovery, the system skips devices that have already been discovered and associated with a site. The system does not assign them to a site again.
- CLI credentials are not required to discover hosts. The system discovers hosts through the network devices they are connected to.
- During discovery using SNMPv3 credentials, Catalyst Center pushes the SNMPv3 credentials with the default SNMP user group to the devices ignoring the existing user group on the device.
- If you choose **Discover new devices only**, the discovery adds only the new devices to the inventory. The discovery does not update any information for existing devices in the inventory.

Discover your network using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, CIDR, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see Discover your network using an IP address range or CIDR, on page 68 and Discover your network using LLDP, on page 70.

Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in Discovery prerequisites, on page 56.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, select **CDP**.

c) In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.

d) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 20 to 32.

e) Click .

Repeat Step d and Step e to exclude multiple subnets from the Discovery job.

f) (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, CDP level 3 means that CDP will scan up to three hops from the seed device.

g) For **Preferred Management IP**, select one of these options:

Option	Description
None	Allows the device to use any of its IP addresses.
Use Loopback IP	Specify the device's loopback interface IP address. **Note** If you select **Use Loopback IP** and the device does not have a loopback interface, Catalyst Center selects a management IP address using the logic described in Preferred management IP addresses, on page 63. **Note** To use the loopback interface IP address as the preferred management IP address, make sure that the CDP neighbor's IP address is reachable from Catalyst Center.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 57.

a) In the left pane, click **CLI** to add CLI credentials.
b) Expand **SNMP** to add SNMP credentials.
c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.
c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy, on page 240.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Discover your network using an IP address range or CIDR

You can discover devices and hosts using an IP address range, CIDR, CDP, or LLDP. This procedure explains how to perform discovery using an IP address range or CIDR. For more information about the other Discovery methods, see Discover your network using CDP, on page 66, and Discover your network using LLDP, on page 70.

Before you begin

Your devices must have the required device configurations, as described in Discovery prerequisites, on page 56.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, choose **IP Address/Range**, or **CIDR**.

c) If you choose **IP Address/Range** discovery type, do these steps:

1. In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Catalyst Center to scan, and click .

   You can enter a single IP address range or multiple IP addresses for the discovery scan.

Note Cisco Wireless Controllers must be discovered using the Management IP address instead of the Service Port IP address. If not, the related wireless controller 360 and AP 360 pages will not display any data.

2. (Optional) To enter additional IP address ranges, repeat the previous step.

d) If you choose **CIDR** discovery type, do these steps:

1. In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.
2. In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

   You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 20 to 32.

3. Click .

   (Optional) To exclude additional subnets from the Discovery job, repeat the previous steps.

4. In the **Prefix Length** field, enter a value between 20 and 30.

e) For **Preferred Management IP Address**, select one of these options:

- **None**: Allows the device to use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose **Use Loopback IP** and the device does not have a loopback interface, Catalyst Center chooses a management IP address using the logic described in Preferred management IP addresses, on page 63.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 57.

a) In the left pane, click **CLI** to add CLI credentials.
b) Expand **SNMP** to add SNMP credentials.
c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.

c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy, on page 240.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

The status of the task displays in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Discover your network using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, CIDR, or an IP address range. This procedure describes how to discover devices and hosts using LLDP. For more information about the other discovery methods, see Discover your network using CDP, on page 66 and Discover your network using an IP address range or CIDR, on page 68.

Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are unnecessary for host discovery. The system discovers hosts by using the network devices they are connected to.

Before you begin

- Enable the LLDP protocol on your network devices.
- Configure your network devices according to Discovery prerequisites, on page 56.
- Configure your network device host IP address as the client IP address. A host is an end-user device, such as a laptop computer or mobile device.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, select **LLDP**.

c) In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.

d) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

Enter addresses as individual IP addresses (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*). In a CIDR address, *x.x.x.x* refers to the IP address, and *y* refers to the subnet mask. The subnet mask can be a value from 20 to 32 bits.

e) Click .

Repeat both Step c and Step d to exclude multiple subnets from the Discovery job.

f) (Optional) In the **LLDP Level** field, enter the number of hops from the seed device to scan.

Valid values are from 1 to 16. The default value is 16. For example, LLDP level 3 means that LLDP scans up to three hops from the seed device.

g) For **Preferred Management IP**, select one of these options:

- **None**: Allows the device use any of its IP addresses.
- **Use Loopback IP**: Specify the loopback interface IP address for the device.

Note If you select this option and the device does not have a loopback interface, Catalyst Center selects a management IP address using the logic described in Preferred management IP addresses, on page 63.

Note To use the loopback interface IP address as the preferred management IP address, make sure that the IP address of the LLDP neighbor is reachable from Catalyst Center.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 57.

a) In the left pane, click **CLI** to add CLI credentials.
b) Expand **SNMP** to add SNMP credentials.
c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.
c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy, on page 240.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Manage Discovery jobs

These sections provide information about how to manage the Discovery jobs.

Stop and start a Discovery job

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To stop an active Discovery job, hover your cursor over the ellipsis icon (•••) in the **Actions** column and select **Stop Discovery**.

Step 3 To restart an inactive Discovery job, hover your cursor over the ellipsis icon in the **Actions** column and select **Re-discover**.

Change credentials in a Discovery job

Change the credentials used in a Discovery job, and rerun the Discovery job.

Before you begin

Create at least one Discovery job before starting.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To copy a Discovery job, hover your cursor over the ellipsis icon (***) in the **Actions** column and choose **Copy & Edit**.

Catalyst Center creates a copy of the Discovery job, named "Clone of *Discovery_Job*."

Step 3 (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.

Step 4 In the **New Discovery** window, expand the **Credentials** area and choose any of the global credentials that have already been created, or configure your own.

To use existing credentials, select them. To exclude a credential, deselect it.

Step 5 To configure your own credentials, click **Add Credentials**.

You must configure CLI and SNMPv2c credentials. Other credentials are optional. For information about each field, see Discovery credentials, on page 57.

To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 6 Click **Discover**.

Clone a Discovery job

You can clone a Discovery job to retain all the information defined for that job.

Before you begin

Ensure you have run at least one Discovery job.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To copy a Discovery job, hover your cursor over the ellipsis icon (***) in the **Actions** column and select **Copy & Edit**.

Catalyst Center creates a copy of the Discovery job named "Clone of *Discovery_Job*."

Step 3 (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.

Step 4 Define or update the parameters for the new Discovery job.

Delete a Discovery job

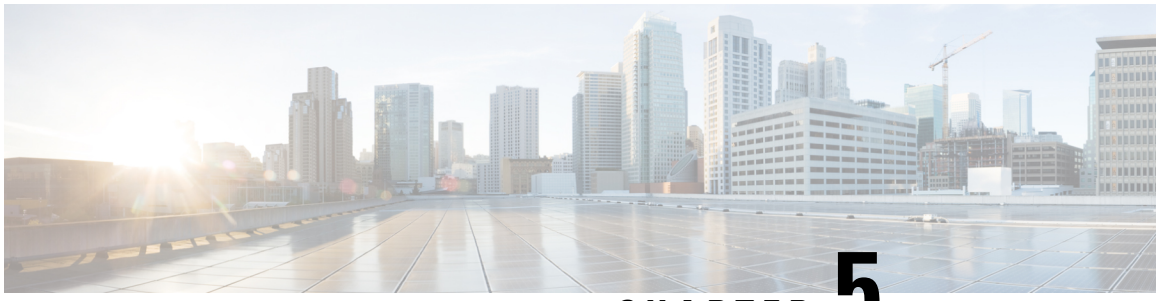
You can delete a Discovery job regardless of whether it is active or inactive.

Procedure

Step 1 From the main menu, choose **Tools** > **Discovery**.

Step 2 To delete a Discovery job, hover your cursor over the ellipsis icon (•••) in the **Actions** column and select **Delete**.

Step 3 Click **OK** to confirm.



CHAPTER 5

Manage Your Inventory

- About Inventory, on page 78
- Inventory and Cisco ISE authentication, on page 79
- Display information about your inventory, on page 80
- Manage user-defined fields, on page 126
- Launch Topology map from Inventory, on page 127
- Types of devices in the Catalyst Center Inventory, on page 128
- Filter devices, on page 154
- Manage devices in the Inventory window, on page 156
- Configure a REP ring for devices, on page 162
- Add a node to a REP ring for nonfabric deployment, on page 164
- Delete a node from a REP ring for nonfabric deployment, on page 165
- MRP ring for nonfabric deployment, on page 166
- View MRP ring topology overlay, on page 167
- View MRP ring status for nonfabric deployment, on page 168
- Parallel redundancy protocol, on page 170
- View the PRP topology status, on page 171
- Create port groups, on page 172
- Assign tags to ports, on page 173
- Port use information, on page 173
- Maintenance mode for devices, on page 174
- Inventory Insights, on page 177
- Manage system beacon, on page 178
- Device roles, on page 179
- Change the device role manually, on page 180
- Update a device management IP address, on page 181
- Update the device polling interval, on page 181
- Resynchronize device information, on page 182
- Delete a network device, on page 183
- Launch Command Runner (Inventory), on page 184
- Troubleshoot device reachability issues using Run Commands, on page 184
- Use a CSV file to import and export device configurations, on page 185
- Configuration drift of a device, on page 189
- View configuration drift of a device, on page 190

• Label configuration drift, on page 192
• Visibility and control of device configurations, on page 193
• Deploy your device configurations now or later, on page 199
• Preview and deploy your device configurations, on page 200
• Network provisioning prechecks, on page 202
• Replace a faulty device, on page 205
• Replace a faulty access point, on page 211
• Manage Out-of-band RMA device replacement, on page 213
• Limitations of the RMA workflow in Catalyst Center, on page 214
• Reboot an access point, on page 216

About Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

The Inventory feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device.

Inventory uses these protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
- LLDP Media Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see Discovery prerequisites, on page 56.

After the initial discovery, Catalyst Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see Update the device polling interval, on page 181. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes. A configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Device resynchronization is also triggered after the inventory service restart under these circumstances:

- If there is an upgrade (Catalyst Center upgrade) after the inventory service restart.
- If the device synchronization is in terminated or delayed state after the service restart.
- If the **Last Sync** time for the device is more than 75 percent of the periodic resync interval configured on the device. For example, after the inventory service restart, if the **Last Sync** time for a device has crossed 18 hours and the configured periodic resync interval is 24 hours, the device will be resynchronized before the periodic resync interval. The percentage for the resync interval cutoff time may vary based on the value configured on the device.

Note Points regarding device resynchronization include:

- Port up/down events are grouped together every 80 seconds. As a result, only one event is reported per 80-second window for each device. This process updates the device's port-related inventory data.
- Configuration change events are grouped every 10 minutes, triggering a resync request for the device.
- If three consecutive syncs occur due to port up/down traps or configuration change traps, the next event-based sync for that device is delayed by 5 minutes.
- If the rate of event bursts exceeds 60% within a consolidation window, the resync for that device is delayed by 45 minutes.

Inventory and Cisco ISE authentication

Cisco ISE has two different use cases in Catalyst Center:

- If your network uses Cisco ISE for device authentication, you need to configure the Cisco ISE settings in Catalyst Center. As a result, when provisioning devices, Catalyst Center configures the devices with the Cisco ISE server information that you defined. In addition, Catalyst Center configures the devices on the Cisco ISE server and propagates subsequent updates to the devices. For information about configuring Cisco ISE settings in Catalyst Center, see Configure global network servers, on page 321.

Note If you are using Cisco ISE for authenticating Cisco Catalyst 9800 series devices, you must configure Cisco ISE to provide privilege for NETCONF users.

If a device is not configured or updated on the Cisco ISE server as expected due to a network failure or the Cisco ISE server being down, Catalyst Center automatically retries the operation after a certain wait period. However, Catalyst Center does not retry the operation if the failure is due to a rejection from Cisco ISE, as an input validation error.

When Catalyst Center configures and updates devices in the Cisco ISE server, the transactions are captured in the Catalyst Center audit logs. You can use the audit logs to help troubleshoot issues related to the Catalyst Center and Cisco ISE inventories. You can also find information on the ISE integration status in the provisioning summary for the device and under the **Provisioning Status** column in Catalyst Center inventory (by clicking the **See Details** link).

After you provision a device, Catalyst Center authenticates the device with Cisco ISE. If Cisco ISE is not reachable (no RADIUS response), the device uses the local login credentials. If Cisco ISE is reachable, but the device does not exist in Cisco ISE or its credentials do not match the credentials configured in Catalyst Center, the device does not fall back to use the local login credentials. Instead, it goes into a partial collection state.

To avoid this situation, make sure that before you provision devices using Catalyst Center, you have configured the devices in Cisco ISE with the same device credentials that you are using in Catalyst Center. Also, make sure that you configured valid discovery credentials. For more information, see Discovery credentials, on page 57. Any deviation in the Cisco TrustSec (CTS) credentials on the device is identified during compliance check and is displayed under the **Network Settings** tile in compliance summary.

- If required, you can use Cisco ISE to enforce access control to groups of devices.

Display information about your inventory

You can display and filter for information about discovered devices in your inventory. You can also customize or change the information displayed in the **Devices** table.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information from the discovery process.

Note For the devices that are added as Fully Qualified Domain Name (FQDN), hover your cursor over the **i** icon next to the device name in the **IP address** column to view the **Resolved IP Address**.

If the **Inventory** window contains APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In this dialog box, you have the option to:

Option	Task
Skip this dialog box in the future.	Check the **Don't show this again** check box.
Open the **License Manager** window and enable the licenses.	Click **License Manager** (for more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*)
Enable the licenses later.	Click **Do this later**.

Step 2 (Optional) To change the site, click **Global** and use either the search bar or network hierarchy to find a site.

The **Inventory** window displays the devices available in the chosen site.

Step 3 (Optional) To change the Inventory view, use the toggle button ( ) in the top-right corner.

You can change your default view (the list layout) to other layouts, such as the topology, or map layout.

Step 4 (Optional) To change the **Devices** table focus views, from the **Focus** drop-down list, select a view, such as **Default**, **Inventory**, or **Software Images**.

Note

- The displayed columns change depending on the chosen focus view.
- The selected devices persist in each new focus view.

Step 5 (Optional) To filter for specific device details in the **Devices** table, use these filter options.

Option	Task
To filter for a device family	Select one or more of the device family buttons at the top of the **Inventory** window. For example, you can click **Routers** to display only routers in the table.
To filter for device work items, in the left pane	Check the check box of one or more work items. The table is immediately filtered for the work item. For example, you can check the **Unreachable** check box to display only unreachable devices in the table.
To filter for specific device details	Click **Filter devices** and select from these options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Then click **Apply**.

For more information, see Filter devices, on page 154.

Step 6 (Optional) To take a guided tour of the **Inventory** window, click **Take a tour** in the top-right corner.

Step 7 (Optional) To export all the data in the **Devices** table, click **Export** in the top-right corner.

Step 8 (Optional) To customize the **Devices** table, click the settings icon (⚙) in the top-right corner, select your preferred options in the **Table Settings** slide-in pane, and then click **Apply**.

Option	Description
Table Appearance	Select to use the default or compact table view and table striping.
Edit Table Columns	Select to create a custom view and to hide or display columns.

Note The column selection doesn't persist across sessions.

This table provides key information about specific table columns.

Column	Description
Device Name	Name of the device. Click the device name to view more information about that device. **Note** If a device name appears in red, the inventory has not polled the device or updated its information for over 30 minutes.

Support Type	Shows the device support level:
	• **Supported**: The device profile is tested for all applications on Catalyst Center. You can open a service request if any of the Catalyst Center functionalities for these devices don't work.
	• **Limited**: The device profile for legacy devices is tested only for these features and tested only on a best-effort basis on Catalyst Center.
	  • Discovery
	  • Topology
	  • Device Reachability
	  • Config Change Audit
	  • Inventory
	  • Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.)
	  • Template Provisioning (Applicable only for switches.)
	For more information, see the *Legacy Device Compatibility Matrix*.
	• **Third Party**: The device profile has been tested on Catalyst Center for third-party devices that are capable of populating SNMP MIB 2 values. Catalyst Center supports limited base automation (Inventory and Topology) and limited assurance capabilities, such as third-party device 360, device health calculation based on reachability status, and device interface and reachability issues.
	For more information, see the *Cisco Catalyst Center Compatibility Matrix*.
	• **Unsupported**: All remaining Cisco and third-party devices that aren't tested and certified on Catalyst Center. You can try out various functionalities on Catalyst Center for these devices, as a best effort. However, you can't raise a service request or a bug if Catalyst Center features don't work as expected.

Reachability	Shows various statuses: • **Reachable**: The device is reachable by Catalyst Center using SNMP, HTTP(S), and NETCONF polling. • **Ping Reachable**: The device is reachable by Catalyst Center using ICMP polling and not reachable using SNMP, HTTP, HTTPS, and NETCONF polling. • **Unreachable**: The device isn't reachable using SNMP, HTTP, HTTPS, NETCONF, or ICMP polling.

Column	Description
EoX Status	Shows the EoX scan status: • **Success**: The device is scanned for EoX alerts successfully. • **Not Scanned**: The device isn't scanned for EoX alerts. • **Scan Failed**: Catalyst Center isn't able to scan the device for EoX alerts. • **Scanning**: Catalyst Center is scanning the device for EoX alerts. Hover your cursor over the **i** icon next to **EoX Status**, and click **Consent to Connect** hyperlink. To initiate an EoX scan, you must accept and submit the authorization in the **Consent to Connect** dialog box. For the devices that are scanned successfully, the **EoX Status** column shows the number of alerts, if any. Click the number of alerts to view the alerts in detail. In the slide-in pane, click the **Hardware**, **Software**, and **Module** tabs to view the hardware, software, and module EoX alerts. **Note** The EoX feature doesn't support scanning APs for EoX alerts.
Manageability	Shows the device status: • **Managed with green tick icon**: Device is reachable and is fully managed. • **Managed with orange error icon**: Device is managed with some error, such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. Hover your cursor over the error message to view more details about the error and the impacted applications. **Note** If the verification of a device's SSH key failed, see Deal with SSH key verification errors, on page 161 for a description of how to deal with this issue. • **Unmanaged**: Device can't be reached and no inventory information was collected because of device connectivity issues. **Note** For an ongoing device resynchronization, the **Syncing** status is displayed. Click the status to view: • Ongoing sync details, • Previous sync details, • Reasons for the synchronization, and • The application that requested the synchronization. A message is displayed for pending resync requests that are in the queue. If multiple requests are pending, they are merged based on the features to be synced and the priority. The sync details can display multiple reasons for a sync event.
Platform	Cisco product part number

Column	Description
Device Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Catalyst Center is unable to determine a device role, it sets the device role to Unknown. **Note** If you manually change the device role, the assignment remains static. Catalyst Center doesn't update the device role even if it detects a change during a subsequent device resynchronization. If required, you can use the drop-down list in this column to change the assigned device role.
Site	The site to which the device is assigned. If the device isn't assigned to any site, do these steps: **a.** Click **Assign**. **b.** Click **Choose a Site**. **c.** Select a site from the hierarchy. **d.** Click **Save**. For more information, see Network hierarchy, on page 229.
Last Updated	Most recent date and time on which Catalyst Center scanned the device and updated the database with new information about the device. **Note** Click **Sync Details** to view the **Last Sync Start Time** and **Reason(s) for Last Sync**. For an ongoing device resynchronization, **Sync Details** displays: • Ongoing sync details, • Previous sync details, • Reasons for the synchronization, and • The application that requested the synchronization. A message is displayed for pending resync requests that are in the queue. If multiple requests are pending, they are merged based on the features to be synced and the priority. The sync details can display multiple reasons for a sync event.
Resync Interval	The polling interval for the device. Set the resync interval from the **Inventory** window by choosing **Actions** > **Edit Device** > **Resync Interval**. To set the resync type as **Global**, from the main menu, choose **System** > **Settings**. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Column	Description
Provisioning Status	Shows the status of the last provisioning operation attempted on a device. Click **See Details** to view the status of past provisioning operations. • **Success**: The latest operation on the device was successful. • **Success with a warning icon**: The latest operation on the device was successful, but there are failures from past provisioning operations that may need user attention. • **Failed**: The latest operation on the device has failed. • **Failed with a warning icon**: The latest operation on the device has failed, and there are failures from past provisioning operations that may need user attention. • **Configuring**: The device is currently being configured. • **Pending**: The system is trying to determine if the device will be impacted by an ongoing provisioning operation. • **Not Provisioned**: The device has never been provisioned. • **Out of Sync**: The network settings or network profiles for a device have been modified after the last provisioning operation. IPv6 devices can be marked as Out of Sync.
Credential Status	Shows the device credential status: • **Not Applied**: The device credential isn't applied on the device. • **Success**: The device credential is applied on the device successfully. • **Failed**: The device credential failed on the device. Click **See Details** to view the details about the credentials. The **Credential Status** slide-in pane shows the **Type**, **Name/Description**, **Status**, and **Details** of the credential. For a device whose status is **Failed**, hover your cursor over the ellipsis icon (***) in the **Actions** column and select **Retry** or **Clear**. • **Retry**: Applies the credential on the device. • **Clear**: Clears the device credential.
AP CDP Neighbors	Displays details about the switch and port connected to an AP in the **Inventory** window. This window displays information about AP CDP neighbors even if the connected access switch is managed by Catalyst Center.

- **Edit Custom Views**: First you must create a custom view in the **Edit Table Columns** tab, and then you can edit the custom view.
- **Reset All Settings**: Reset the table settings to the default settings.

Step 9 (Optional) To manage your devices from the **Devices** table, you can tag devices, add devices, or use the **Actions** drop-down list.

Name	Description
Tag	Click **Tag** to tag devices, edit tags, delete tags, or create port group. For more information, see Manage devices in the Inventory window, on page 156.
Add Device	Click **Add Device** to add a network device, add a compute device, or integrate a Meraki dashboard or Firepower Management Center (FMC) with Catalyst Center. For more information, see Types of devices in the Catalyst Center Inventory, on page 128.
Actions drop-down list	Use the **Actions** drop-down list to manage your devices, software images, telemetry, and more. To view more details about each action option, click the right-adjacent information icon (ⓘ).

Step 10 (Optional) In the **Devices** table, you can do a variety of actions.

- To sort the columns in either ascending or descending order, click the column header.
- To view more details about a device, click the device name and then click **View Device Details**.
- To view a device's compliance details, click either **Non-Compliant** or **Compliant** under the **Compliance** column.
- To assign a site to a device, click **Assign** under the **Site** column.
- To change a device role, click the edit icon under the **Device Role** column and then select from the options, such as **ACCESS** or **CORE**.
- To change the number of entries, scroll down to the bottom of the window, and from the **Show Records** drop-down list, select the number of entries that you want to appear.

Note If there are more than 25 entries in the table and you select a different focus view, the same number of entries appears in each new view.

Note Each focus view displays different columns, and you can customize a table view to include columns, such as **Compliance**, **Site**, **Device Role**, and **Software Image**.

Display information about a device

You can display, filter, and search for information about a discovered device, its security, and its compliance.

Before you begin

Make sure that you have devices in your inventory; otherwise, use the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays information about devices that you discovered.

Step 2 In the **Devices** table, click the name of a device to view more information about it.

Step 3 Click **View Device Details**.

The device details display in the window.

Step 4 Use this table that describes the available information in this window to display, filter, and search for details about a device.

Name	Description
Run Commands	This link is available only for routers, wireless controllers, switches, and hubs. Launch the Command Runner application to run diagnostic CLI commands and view the resulting command output on a device.
Manage APs	This link is available only for Cisco Catalyst 9800 Series Wireless Controllers on which the Per-Device Configuration feature is enabled. For a wireless controller that is provisioned using Per-Device Configuration, click this link to manage the associated APs. **Note** If the wireless controller is provisioned using the intent-based wireless network configurations with site-based network profiles, you can only view the list of associated APs using this link. For more information, refer to Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller, on page 676.
View 360	This link is available for all devices. Displays the **Device 360** window for that device. To open this window, you must have installed the Assurance application.
Interfaces	This feature is available for all devices except APs. Displays information about the device's ports, such as its Ethernet ports, in a topology or table view. You can view the settings under the **Details** tab. For more information about device interfaces, refer to Display information about a device interface, on page 92.

Name	Description
Hardware & Software	This feature is available on all devices. Displays the device's hardware and software details, such as its uptime, provision status, and Cisco ISE integration status, with an operational summary.
Configuration (running configuration)	This feature is available only for APs, routers, and switches. Go to **Details** > **Browse configurations** to view the settings. For routers, switches, and hubs, this option displays detailed configuration information that is similar to what is displayed in the output of the **show running-config** command. You can hide line numbers, search for a command line or piece of text, or export the CLI output. For APs, this tab displays information about the AP configuration and radio configurations. This feature is not supported for wireless controllers, so configuration data is not returned for this device type.
Power	This feature is available only for routers and switches. Displays details about the device's power usage and power supplies. Go to **Details** > **System** to view the settings. Enter values in the **Name**, **Operational Status**, and other fields to search and filter the data in the **Power Supplies** table. The narrowed search results display with the matching values highlighted throughout the table.
Fans	This feature is available only for routers and switches. Displays details about fans. Go to **Details** > **System** to view the settings. Enter values in the **Name**, **Operational Status**, and other fields to search and filter the data in the **Fans** table. The narrowed search results display with the matching values highlighted throughout the table.
SFP Modules	This feature is available only for routers and switches. Displays details such as the manufacturer and the ports to which the Small Form-Factor Pluggable (SFP) modules are connected. Go to **Details** > **System** to view the settings. Enter values in the **Name**, **Platform**, and other fields to search and filter the data in the **SFP Modules** table. The narrowed search results display with the matching values highlighted throughout the table.

Name	Description
User Defined Fields	This feature is available for all devices. Displays the user-defined fields associated with the device. You can view the settings under the **Details** tab. Click **Manage User Defined Fields** to display the **Manage User Defined Fields** slide-in pane. You can do these tasks: • Click **Create New Fields** to create a new field. • Click **Search Table**, manually enter a value, and then press the **Enter** key. The narrowed search results display with the value highlighted throughout the table. To add a user-defined field to a device, you must first create a user-defined field in the **Manage User Defined Fields** slide-in pane. For more information, refer to Create user-defined fields, on page 126. Assign the user-defined field to a device and add a value to display it. For more information, refer to Add user-defined fields to a device, on page 127.
Config Drift	This feature is available for all devices. Displays configuration changes on the device, including a change history, and compares two configuration versions. You can do these tasks: Go to **Details** > **Browse configurations** to view the settings. • Label the configuration drift on the time line for future reference. For more information, refer to Label configuration drift, on page 192. • Pick any two versions of the same device and compare their running configuration data.
REP Rings	This tab is available for Cisco Catalyst Industrial Ethernet 3100, 3200, 3300, 3400, 4000, 5000, and 9300 Series Switch. Cisco Embedded Services 3300 Series Switches (ESS3300), S5200, and S5800. Displays details about Resilient Ethernet Protocol (REP) rings, such as its name, ring size, first adjacent device, and so on. You can view the settings under the **Redundancy** tab. Click **Create REP Ring** and follow the workflow to create a REP ring. For more information, refer to Delete a node from a REP ring, on page 1067 or Delete a REP ring, on page 1066.

Name	Description
MRP Rings	This tab is available only for Cisco Industrial Ethernet (IE) 3000, 4000, 5000 Series Switches. Displays details about Media Redundancy Protocol (MRP) rings, such as ring ID, ring size, VLAN ID, network topology status, profile value, and ring details. You can view the settings under the **Redundancy** tab. To view the MRP ring details from **Provision** > **Inventory** > **Topology** view, click anywhere on the ring. For more information, refer to MRP ring for nonfabric deployment, on page 166 and View MRP ring status for nonfabric deployment, on page 168.
Wireless Info	This tab is available only for wireless controllers. View details about managed sites, wireless settings, redundancy, health parameters, and other information. In the **Wireless Summary** tab, in the **SSIDs** table, you can search for a specific value by clicking **Search Table**, manually entering a value, and then pressing the **`Enter`** key. The narrowed search results display with the value highlighted throughout the table.

Name	Description
Configuration (per-device configuration)	This area is available only for wireless controllers and switches. **Wireless controller:** • **Mobility**: This tab displays mobility details, such as the mobility group name, RF group name, and so on. The **Mobility Peers** table displays if mobility peers are configured on the device. If mobility peers are not configured, refer to Configure mobility group, on page 650. You can filter the table to display specific mobility peers by any combination of values, such as values for **MAC address**, **Device Name**, and **IP Address** fields. • Per-Device Configuration: Available only for Cisco Catalyst 9800 Series Wireless Controllers on which this feature is enabled. For the wireless controller, you can use Per-Device Configuration to manage individual features such as, WLAN configurations, RF configurations, and so on. **Note** If the wireless controller is provisioned using the intent-based configurations with site-based network profiles, you can only view the device configurations in this area. For more information, refer to Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 672. **Switches**: Displays the per-device configurations for Cisco Catalyst Switches. This feature is available for Cisco Catalyst 9000 Series Switches and Cisco Catalyst Industrial Ethernet (IE) Switches running Cisco IOS XE Release 17.12.x and later. For more information, refer to Manage per-device configurations for Cisco Catalyst Switches, on page 96.
Security	This tab is available for all devices. View a device's advisory details in the **Advisories** table. You can do these tasks: • Click **Manage All** to display the **Security Advisories** window to manage your devices and advisories. • Click **Filter** to display advisories by any combination of values, such as values for the **Advisory ID** and **Advisory Title** fields. Then click **Apply**. • Click an advisory ID to display more information about that advisory. • In the **Custom Match Pattern** column, click **Add match pattern** to add or update a condition to match with devices in the **CONDITIONS** text box. Then you can save the match pattern and run a scan to check the number of devices that match with the match pattern.
Field Notices	Displays information about field notices for the device. Refer to View Field Notices.

Name	Description
Potential Field Notices	Displays information about potential field notices for the device.
Compliance	This tab is available for all devices. Displays a device's compliance summary, such as when compliance last ran for the Startup vs Running configuration. You can do these tasks: • Click **Run Compliance Check** to check the device for compliance. • Click **View Preference for Acknowledged Violations** to view the list of acknowledged violation attributes. You can unlist a violation to open it.

Display information about a device interface

For routers, wireless controllers, switches, or hubs, you can display, search, and filter for information about a device's interface. Depending on the device, certain information is available.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 In the **Devices** table, click the name of a device, and then click **View Device Details**.

Step 3 Click **Details** > **Interfaces**.

Step 4 Use this table that describes the **Interfaces** drop-down list options to display details about an interface.

Name	Description

Ethernet Ports	• This tab is available for all devices except APs.
	For routers and switches, port information is displayed under the **Summary** tab.
	• Ethernet port details appear in two views: topology and table.
	  • The topology view displays the Ethernet port topology of a device with a color-coded system of each port's connection status.
	  • The table view shows Ethernet port details, such as operational status and admin status.
	• For more information about the two views, see Display information about Ethernet ports, on page 93.

Name	Description

VLANs	• This tab is only available for switches and hubs.
	• Displays VLAN details, such as its operational status and admin status, in table format.
	• The **VLANs** table displays the ID of these types of VLANs:
	  • VLAN ID of the manufacturing-supplied default VLAN
	  • VLAN ID of the configured default VLAN
	  • VLAN ID of the configured VLAN
	Enter values in the **Name**, **Operational Status**, and other fields to search and filter the data in the **VLANs** table. The narrowed search results display with the matching values highlighted throughout the table.

Virtual Ports	• This tab is only available for wireless controllers and routers. • Displays details about ports, such as the operational status, admin status, and so on. • Enter values in the **Name**, **Operational Status**, and other fields to search and filter the data in the **Virtual Ports** table. The narrowed search results display with the matching values highlighted throughout the table.

Display information about Ethernet ports

Use this procedure to display, search, and filter for certain information about a port or ports through either the topology view or table view.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Devices** table, click a device name, and then click **View Device Details**.

Step 3 Click **Details** > **Interfaces** > **Ethernet Ports**.

For routers and switches, port information is displayed under the **Summary** tab.

Step 4 In the upper-right corner, click **Topology View** () to view the Ethernet port topology if it's not already displayed.

This view displays the Ethernet port topology of a device with a color-coded system of each port's connection status. Hover your cursor over a port for more details.

Note For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series Switches and Cisco ASR 1000 Series Aggregation Services Routers, this view displays line cards and supervisor cards details, such as the part number and serial number, if the cards are available.

Step 5 In the topology view, you can do these tasks:

- To view the error reason for an error-disabled port, click the port.
- To filter for a specific Ethernet port, use the **Color Code** drop-down list. The table describes the available drop-down list options.

Table 11: Color code drop-down list options

Name	Description
Status	Displays the default view of the topology view.
Access VLANs	Displays the access VLAN assigned to a particular port. The Access VLANs view allows you to select a maximum of five access VLANs and lists only the access VLANs associated with the port. This option displays the access VLANs in this color-coded system: **Selected**, **Not Configured**, **Default**, and **VLAN**.
Port Channels	Displays the top five port channels that are configured on the device. This option only displays the configured port channels on the device in this color-coded system: **Selected** and **Port-channel** with a corresponding number.

Step 6 In the upper-right corner, click **Table View** ( ) to view the **Ports** table.

The **Ports** table displays Ethernet ports details, such as a ports' operational status, admin status, and so on.

Step 7 (Optional) Enter values in the **Port name**, **Operational status**, **Tags**, and other fields to search and filter the data in the **Ports** table. The narrowed search results display with the matching values highlighted throughout the table.

Step 8 (Optional) In the table view, you can do these tasks:

- Click **Tag** to tag a port or ports, search for a tag, or manage tags.

  For more information, see Assign tags to ports, on page 173.
- Click **Export** to export the **Ports** table data.

Manage port details

Use this procedure to manage and edit port details of a device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Devices** table, click a device name, and then click **View Device Details**.

Step 3 Click **Details**.

Step 4 In the left pane, expand **Interfaces** and choose **Ethernet Ports**.

Step 5 In the topology view ( ), click a port. In the table view ( ), click a port name.

Note

- For Catalyst 2000, 3000, and 9000 Series Switches, port details include the port's maximum allocated power and power drawn.
- This window shows CDP neighbor details. If CDP is absent, LLDP neighbor details appear. If neither CDP nor LLDP neighbors are present, the **Neighbor Details** area is hidden.
- For Cisco Catalyst 9000 Series Switches and Cisco Catalyst IE Switches running Cisco IOS XE Release 17.12.x and later, the per-device configurations for the port are displayed.

Step 6 (Optional) To tag the port, search for tags, manage tags, or create a new tag, click **Tag**.

For more information, see Assign tags to ports, on page 173.

Step 7 (Optional) To manage the port, click the **Port Actions** drop-down list and choose from these options:

- To shut down the port and change the port's admin status to Down, select **Port Shut**. Then click **Okay** to confirm.

  This option is only available when the port is open and the admin status is Up.
- To open the port and change the port's admin status to Up, select **Port No Shut**. Then click **Okay** to confirm.

  This option is only available when the port is shut and the admin status is Down.
- To clear the port's MAC address, select **Clear Mac Address**.
- To activate an error-disabled port, clear the MAC address, and shut down the port.

Note

- The device software type must be Cisco IOS or Cisco IOS XE to clear the MAC address and shut down a port.
- For wireless controllers, clearing the MAC address and shutting down the port are not supported.
- Clearing the MAC address and shutting down the port are supported only on access ports.
- Shutting down a port disrupts traffic on that port.

Step 8 Use this table to edit port details, such as the port description area.

Name	Description
Access VLAN	Click the **Edit** icon. In the **Edit Access VLAN** dialog box, choose an access VLAN from the drop-down list, and then click **Save** to assign the access VLAN to the port. If a port has two access VLANs preconfigured, you cannot update its access VLAN.
Voice VLAN	Click the **Edit** icon next to **Voice VLAN**. In the **Edit Voice VLAN** dialog box, choose a voice VLAN from the **Select Value** drop-down list, and then click **Save** to assign the voice VLAN to the port.
Port Description	Click the **Edit** icon next to **PORT DESCRIPTION**. Enter a description. Click **Save**. Click **Okay** to add a description to the port. Click the delete icon to delete the description. When prompted in the **Warning** dialog box, click **Okay**.

Note

- The device software type must be Cisco IOS or Cisco IOS-XE to edit VLAN details and the port description.
- Editing VLAN details is supported only on access ports.
- For wireless controllers, editing VLAN details is not supported.

Step 9 (Optional) In the **Configurations** area, click **Edit** to modify the per-device configurations for the port. (For Cisco Catalyst 9000 Series Switches and Cisco Catalyst IE Switches)

Manage per-device configurations for Cisco Catalyst Switches

This section explains how to view and edit the per-device configurations of Cisco Catalyst switches. The configurations described here are supported on Cisco Catalyst 9000 Series Switches and Cisco Catalyst Industrial Ethernet (IE) Switches running Cisco IOS XE Release 17.12.x and later.

Note

- The supported configurations may vary depending on your device model.
- You cannot edit configurations for devices that are part of a network or device group.
- Supported Cisco Catalyst IE Switches:
  - Cisco Catalyst IE3100 Rugged Series
  - Cisco Catalyst IE3100 Heavy Duty Series
  - Cisco Catalyst IE3200 Rugged Series
  - Cisco Catalyst IE3300 Rugged Series
  - Cisco Catalyst IE3400 Rugged Series
  - Cisco Catalyst IE3400 Heavy Duty Series
  - Cisco IE3500 Rugged Series
  - Cisco IE3500 Heavy Duty Series
  - Cisco Embedded Service 3300 Series Switches
  - Cisco Catalyst IE9300 Rugged Series
  - Cisco Catalyst ESS9300 Embedded Series Switch

For fabric devices, the Edit window displays a notification indicating that the device is part of a fabric network. Fabric device configurations can be edited only when the device is synchronized following its latest provisioning operation. If the device is out of sync, a banner is displayed to resynchronize it before editing.

The table describes feature support for fabric devices.

Features	Support	Description
• STP, UDLD, MAC Address Table • BFD, DHCP Relay, OSPF, Static Routes • QoS • ARP Snooping, Device Tracking	Supported	These features are supported. However, some of their attributes are unsupported. These attributes are disabled and cannot be edited.

Features	Support	Description
• VLAN, CDP, LLDP, VTP, IGMP/MLD Snooping, and EtherChannel • Routing and VRF • DNS, NTP, AAA, and DHCP Server • ACL, 802.1X Authentication, DHCP Snooping, and Cisco TrustSec (CTS)	Unsupported	These features cannot be edited and are available in read-only mode.
• Port-channel • Loopback and SVI	Limited support	Modifications to these features are restricted. You can edit existing instances, but you cannot add or delete them.

Before you begin

Make sure that you have devices in your inventory; otherwise, use the Discovery feature.

Verify that the devices are reachable.

Follow these steps to view and manage your switch configurations.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window shows the device information that is gathered during the discovery process.

Step 2 In the **Devices** table, click the device name, and then click **View Device Details**.

Step 3 Enable per-device configuration if it is not already enabled.

In the **Configuration** window, click **Learn more** and follow the instructions to enable per-device configuration on the device.

Step 4 In the **Configuration** window, view and manage your device configurations, as needed.

Use these options to sort, filter, and export the table data displayed in the configuration details window.

- To sort the columns in either ascending or descending order, click the column header.
- Use the **Search Table** option to search for an item.
- Click the filter icon to display the table items by any combination of values.
- Click **Export** to export the table data.
- Click the settings icon to customize the table.

To edit or add configurations, in the configuration details window, click the **Edit** icon.

You can use these options in the edit windows.

- **Reset** and **Set to Default** options to reset the settings or to restore the default settings.
- The Remove icon to delete a value from a field and the Delete icon to remove a configuration.
- **Add configurations** to configure additional configurations.

View and edit the Layer 2 configuration of a device

Use this procedure to view and edit the Layer 2 configuration of a switch.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.
The **Inventory** window shows the device information that is gathered during the discovery process.

Step 2 In the **Devices** table, click the device name, and then click **View Device Details**.

Step 3 Choose one of these options to view the Layer 2 configuration details.

- In the **Layer 2** area, click **View Layer 2 Details**.
- Click the **Configuration** tab and expand **Layer 2 Configuration**.

Step 4 Refer to the table for guidance about viewing and editing the Layer 2 configurations.

Table 12: Layer 2 configuration details

Name	Description
VLAN	View the list of supported VLANs. Click the VLAN ID to view details. Use these options to add or edit a VLAN: • To add a new VLAN, click **Add VLAN**. Enter the VLAN ID, VLAN Name and add other configurations, if required. • To edit a VLAN, select the check box next to the VLAN ID and click **Edit**. Edit or add other configurations as required.

Name	Description
Discovery Protocols	View the discovery protocol (CDP and LLDP) details. • **Admin Status**: Enable or disable the discovery protocol. • **Hold Time**: Determines the duration for retaining the CDP/LLDP information by neighbors. CDP: Range is 10 to 255, default value is 180. LLDP: Range is 0 to 65535, default value is 120. • **Timer**: Interval for sending the CDP/LLDP packets. CDP: Range is 5 to 254, default value is 60. LLDP: Range is 5 to 65534, default value is 30. • **Advertisement version**: CDP version—V1, V2. Default value is V2. • **Reinitialization Delay**: The time delay for LLDP restart after a configuration change or reset.
STP	View the STP configuration details. • **Mode**: STP mode—Rapid-pvst, mst, pvst. Default value is Rapid-pvst. • **Portfast Mode**: Enable or disable the portfast mode for the device. • **BPDU Filter**: Enable or disable BPDU filtering for portfast ports. Default value is Disabled. • **BPDU Guard**: Enable or disable BPDU guard for portfast ports. Default value is Disabled. • **Backbonefast**: Enable or disable the Backbonefast feature, which enables detection and recovery from indirect link failures. Default value is Disabled. • **Logging**: Enable or disable logging for STP events. Default value is Disabled. • **Uplinkfast**: Enable or disable the Uplinkfast feature, which accelerates connectivity recovery after a link failure. Default value is Disabled. • **Loopguard**: Enable or disable Loopguard for STP. Loopguard protects against accidental loss of BPDUs. Default value is Disabled. • **Transmit Hold Count**: Number of BPDUs transmitted per second. Valid range is 1 to 20 seconds. Default value is 6. • **Uplinkfast Max Update Rate**: Maximum update rate for Uplinkfast in packets per second. Valid range is 0 to 32000. Default value is 150.

Name	Description
VTP	View the VTP details. • **Version**: VTP version—V1, V2, V3. Default value is V1. • **VTP Mode**: VTP mode for the device—Client, Server, Transparent, off. Default value is Server. • **Domain Name**: VTP domain name. The maximum length is up to 32 characters.
IGMP Snooping	View the IGMP Snooping details. • **Admin Status**: Enable or disable IGMP snooping. • **Querier**: Enable or disable querier feature IGMP snooping. • **Querier Address**: IP address of IGMP querier. • **Querier Query Interval**: Interval between IGMP queries. Valid range is 1 to 18000. Default value is 60. • **Querier Version**: IGMP version used by the querier. Valid range is V1, V2, V3. Default value is V2. • **Last Member Query Interval (msec)**: Interval for IGMP last member queries. Value is in milliseconds. Valid range is 100 to 32767. Default value is 1000.
MLD Snooping	View the MLD Snooping details. • **Admin Status**: Enable or disable MLD snooping. • **MLD Query Interval (msec)**: Interval for MLD last listeners. Value is in milliseconds. Valid range is 100 to 32768. Default value is 1000.
UDLD	View the UDLD details. • **Admin Status**: Enable or disable UDLD. • **Aggressive**: Enable or disable aggressive mode for UDLD. • **Message Interval**: Interval between UDLD messages. Value is in seconds. Valid range is 1 to 90. Default value is 15. • **Recovery**: Enable or disable recovery for UDLD. • **Recovery Interval**: Interval for UDLD recovery. Value is in seconds. Valid range is 30 to 86400. Default value is 3000.

Name	Description
MAC Address Table	View the MAC address table settings such as MAC address aging and the notification settings. • **Aging Time**: Specifies the time to retain the MAC address before removing from the table. • **Change Notification**: Enable or disable notifications for MAC address table changes. • **Notification Threshold**: Enable or disable threshold-based notifications for MAC address table. • **MAC Move Notification**: Enable or disable notifications for MAC address moves between interfaces. • **Notification Threshold Interval**: Interval for threshold-based notifications for MAC address table. Value is in seconds. Valid range is 120 to 1000000. Default value is 120. • **Notification Limit Percentage**: Percentage threshold for MAC address table notifications. Valid range is 0 to 100. Default value is 50.
EtherChannel	View the port channel settings. • **System Priority**: System priority for LACP (Link Aggregation Control Protocol). Valid range is 0 to 65535. Default value is 32768. • **Load Balance Method**: Load balancing method for port channel.

Step 5 After editing the required configurations, click **Next**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

View and edit Layer 3 configuration of a device

Use this procedure to view and manage the Layer 3 configurations.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name, then select **View Device Details**.

Step 3 Select an option to view the Layer 3 configuration details.

- Under **Summary**, in the **Layer 3** area, click **View Layer 3 Details**.
- Click **Configuration** and expand **Layer 3**.

Step 4 Refer to the table to view and modify configuration details.

Table 13: Layer 3 configuration details

Name	Description
VRF	View the IPv4 and IPv6 VRFs configured on the device. **IPv4 VRF** • **VRF Name**: Name for the VRF instance. • **Route Distinguisher**: Unique identifier to distinguish routes in different VRFs. • **Route-Target**: Number of configured VRF route targets. **IPv4/IPv6 VRF** • **VRF Name**: Name for the VRF instance. • **Route Distinguisher**: Unique identifier to distinguish routes in different VRFs. • **IPv4**: Enable or disable IPv4 for routing and address assignment. • **IPv6**: Enable or disable IPv6 for routing and address assignment.
Loopback	View the loopback interfaces configured on the device. Select the loopback number to view interface details. • **Loopback Number**: Identifier for the loopback interface. • **Description**: Text description for the interface. • **IPv4 Address**: IPv4 address assigned to the interface. • **IPv4 Subnet Mask**: Subnet mask for the IPv4 address. • **IPv6** : Enable or disable IPv6 on the interface. • **IPv4/IPv6 VRF Name**: IPv4/IPv6 VRF name for the interface. • **IPv4 VRF Name**: IPv4 VRF name for the interface. • **BFD**: Enable or disable Bidirectional Forwarding Detection (BFD) on the interface. • **BFD Template**: Name of the BFD Template applied on the interface. • **BFD Interval Status**: Enable or disable the BFD interval configuration.

Name	Description
SVI	View the switch virtual interfaces (SVI) interface details configured on the device. Select the VLAN number to view the interface details. • **VLAN Number**: Identifier for the interface. Valid range is 1 to 4094. • **Description**: Text description for the interface. • **IP Address Type**: IPv4 address assigned to the interface. • **IPv6** : Enable or disable IPv6 on the interface. • **IPv4/IPv6 VRF Name**: IPv4/IPv6 VRF name for the interface. • **IPv4 VRF Name**: IPv4 VRF name for the interface. • **Admin Status**: Enable or disable the interface. • **BFD**: Enable or disable Bidirectional Forwarding Detection (BFD) on the interface. • **BFD Template**: Name of the BFD Template applied on the interface. • **BFD Interval Status**: Enable or disable the BFD interval configuration.
Routing	View the unicast routing configuration on the device. • **IPv4 Unicast Routing**: Enable or disable IP routing globally. When enabled, the device can forward packets between networks based on routing tables, supporting inter-network communication. • **IPv6 Unicast Routing**: Enable IPv6 unicast routing globally. When enabled, the device can forward IPv6 packets between networks based on routing tables, supporting inter-network IPv6 communication.

Name	Description
Static Routes	View static routes configured on the device. • **IPv4** static routes. • **Prefix**: IP prefix for the static route. • **Prefix Mask**: Subnet mask for the static route. • **Forwarding list**: Number of forwarding lists for the static route. • **IPv4 Per-VRF Name** static route: • **VRF Name**: VRF name for the static route. • **Forward list**: Number of forwarding lists for the static route. • **IPv6**: • **VRF Name**: VRF name for the static route. • **Forward list**: Number of forwarding lists for the static route. • **IPv6 Per-VRF Name** static route • **Prefix**: IP prefix for the static route. • **Forwarding list**: Number of forwarding lists for the static route.
BGP	View BGP community values configured on the device in AS:community format. • **Autonomous System Number**: BGP autonomous system number for the routing process. • **Always Compare MED**: Enable or disable to compare MED values from different neighbouring autonomous systems. • **Deterministic MED**: Enable or disable MED comparison for BGP best-path selection. • **Graceful Restart**: Enable or disable BGP graceful restart for the routing process. • **Graceful Restart Extended**: Enable or disable extended BGP graceful restart when longer route preservation is needed during peer recovery.

Name	Description
OSPF	View OSPF details configured on the device. • **OSPF**: • **Process ID**: OSPF process ID for the routing instance. • **Router ID**: Router ID for the current process. • **BFD All Interfaces**: Enable or disable BFD for all interfaces in this OSPF process. • **Strict Mode**: Enable or disable to make OSPF adjacencies dependent on BFD session state. • **Non Stop Routing**: Enable or disable OSPF Nonstop Routing for this process. • **OSPF Per VRFs**: • **Process ID**: OSPF process ID for the VRF routing instance. • **VRF Name**: VRF name associated with this OSPF process. • **NSR**: Enable or disable OSPF Nonstop Routing for this VRF process. • **BFD**: Enable or disable BFD for all OSPF interfaces in this VRF process. • **Strict Mode**: Strict-mode setting for BFD on all OSPF interfaces. Enable this when OSPF adjacencies should depend on BFD session state. • **OSPFv3s**: • **OSPFv3 ID**: OSPFv3 process ID for this routing instance. • **BFD on All Interfaces**: Enable or disable BFD for all interfaces in this OSPFv3 process. • **LSA Arrival Timer**: Minimum interval between accepted OSPFv3 LSA arrivals. • **LSA Delay Timer**: Initial delay before OSPFv3 generates throttled LSAs. • **LSA Minimum Delay**: Minimum delay between originating the same OSPFv3 LSA.

Name	Description

BFD	View BFD protocol details configured on the device.
	• **IPv6 L3 CoS**: IPv6 Layer 3 Class of Service (CoS) value for BFD packets.
	• **More SNMP Traps**: Enable or disable additional SNMP traps for BFD events.
	• **BFD Template Single Hop**
	  • **Name**: Name for the template.
	  • **Echo**: Enable or disable BFD echo function.
	  • **Minimum Transmit Interval**: Minimum interval between transmitted BFD packets.
	  • **Minimum Receive Interval**: Minimum interval between received BFD packets.
	  • **Interval Multiplier**: Number of missed BFD packets before triggering a failure.
	  • **Authentication Keychain**: Keychain name used for authentication in BFD single-hop template.

DHCP Relay	View the DHCP relay information options. • **Trust All Information**: Option to enable or disable the acceptance of all relay information. • **Insert Information Option**: Enable or disable the default relay information option. • **Insert VPN suboption**: Enable or disable the option to include VPN related information in DHCP relay messages.

Step 5 Click the **Edit** icon to update the configurations.

Step 6 Click **Next** after you edit the required configurations.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

View and edit security configuration of a device

Use this procedure to view and manage the security configuration of a switch.

Before you begin

Make sure that you have devices in your inventory; otherwise, use the Discovery feature.

Verify that the devices are reachable.

You must enable per-device configuration to manage switch configurations. In the **Configuration** window, click **Learn more** and complete the steps to enable per-device configuration on the device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name, then select **View Device Details**.

Step 3 Select an option to view the security configuration details.

- Under **Summary**, in the **Security** area, click **View Security Details**.
- Click the **Configuration** tab and expand **Security**.

Step 4 Refer to the table to view and modify configuration details.

Name	Description
ACL	View a list of ACLs such as IPv4 ACLs, MAC ACLs, and IPv6 ACLs. • **IPv4 Extended Access Lists** • **IPv4 Standard Access List** • **IPv4 Role-Based Access List** • **MAC Access List** • **IPv6 Access List** • **IPv6 Role-Based Access List**
Authentication	View authentication settings. • **Admin Status**: Enable or disable the 802.1x authentication mode. • **Verbose Logging**: Enable or disable verbose logging for 802.1x authentication events. • **802.1x Credentials**: 802.1x authentication credentials.

Name	Description
DHCP Snooping	View DHCP Snooping details, such as status, DHCP snooping VLANs, and other default configurations. • **Snooping**: Enable or disable DHCP Snooping. • **Glean**: Enable or disable gleaning for DHCP snooping information. • **Information Option**: Option for DHCP snooping information. • **DHCP Snooping VLANs**: Number of DHCP snooping VLANs.

CTS	Displays the Cisco TrustSec details.
	• **Device SGT**: SGT number for the incoming traffic. Valid range is
	  • 2 to 65519 (for IOS XE 17.6 or later).
	  • 2 to 65521 (for IOS XE 17.6 or earlier).
	• **Authorization List Name**: Cisco TrustSec global authorization.
	• **Enforcement**: Enable or disable role-based access control. Default value is disabled.
	• **SGT VLAN Map**: View the number of SGT to VLAN mappings. Click the number to view the SGT and the mapped VLANs.
	• **Enforcement VLANs**: View a list of VLANs where SGACL policy is enabled.

ARP inspection	View ARP inspection VLANs. Valid range for VLAN: 1 to 4094.
Device Tracking	View whether tracking is enabled or disabled and lists tracking policies. By default, device tracking is disabled.

Step 5 Click the **Edit** icon to update the configurations.

Note You cannot edit configurations for devices that are part of a network, device group, or Cisco SD-Access fabric network.

Step 6 After editing the required configurations, click **Next**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

View and edit the network settings of a device

Use this procedure to view and manage network settings configured on a switch.

Before you begin

Make sure that you have devices in your inventory; otherwise, use the Discovery feature.

Verify that the devices are reachable.

You must enable per-device configuration to manage switch configurations. In the **Configuration** window, click **Learn more** and complete the steps to enable per-device configuration on the device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name, then select **View Device Details**.

Step 3 Select an option to view the network settings configured on the device.

- Under **Summary**, in the **Network Settings** area, click **View Network Settings**.
- Click **Configuration** and expand **Network Settings**.

Step 4 Refer to the table to view and modify configuration details.

Table 14: Network settings

Name	Description

NTP	View NTP settings configured on the device.
	• **Authenticate**: Enable or disable the NTP authentication. By default, it is disabled.
	• **Logging**: Enable or disable logging for NTP events. By default, it is disabled.
	• **Stratum Number**: Stratum number for NTP master configuration. Valid range is 1 to 15. Default value is 8.
	• **Source Loopback Interface**: Loopback interface for the NTP packets. Valid range is 0 to 2147483647.
	• **NTP Servers**: List of NTP servers.
	  • **NTP Server Address**: IPv4 or IPv6 address of the NTP server.
	  • **Peer Authentication Key**: Authentication key number for NTP server.
	  • **Preferred**: Option to enable or disable the NTP server as a preferred server.
	• **NTP Per VRF Server**: List of NTP Per VRF servers.
	  • **VRF**: VRF name for the NTP server. Maximum length is up to 32 characters.
	  • **NTP Servers**: Number of NTP servers associated with the VRF.
	• **NTP Trusted Key**: Trusted key number for NTP authentication. Valid range is 1 to 65535.
	• **NTP Authentication Key**:
	  • Authentication Key Number: Key number for NTP authentication. Valid range is 1 to 4294967295.
	  • Authentication Key: MD5 configuration string for NTP authentication key. Maximum length is up to 32 characters.

Name	Description
DNS	View DNS settings, such as DNS lookup status, default domain name, and the list of DNS servers. • **DNS Lookup**: Enable or disable DNS domain lookup. • **DNS Query Timeout**: Specifies the time to wait for DNS response before considering the DNS attempt as failed. • **Default Domain Name**: Domain container name. • **Per VRF Default Domain Name**: Number of IP domains (VRF) • **Default Domain Name List**: Domain name for DNS resolution. • **Source Loopback Interface**: Loopback interface used as source for DNS lookup. • **DNS Servers**: List of DNS server IP addresses. • **Per VRF DNS Servers**: Number of Per VRF DNS servers.

Name	Description
DHCP	

Name	Description

	View DHCP settings, such as Ignore BOOTP, IPv4 and IPv6 DHCP pools, and excluded addresses for DHCP.
	• **Ignore BOOTP**: Enable to ignore BOOTP packets in DHCP processing.
	• **IPv4 DHCP Pools**: List of IPv4 DHCP pools.
	  • **DHCP Pool Name**: Unique identifier for the DHCP pool.
	  • **Network**: Network number for the primary DHCP pool.
	  • **Subnet Mask**: Subnet mask for the primary DHCP pool network.
	  • **VRF Name**: VRF name for DHCP pool, enabling logical network segmentation.
	  • **DNS Server**: List of DNS server IP addresses for DHCP clients.
	• **IPv6 DHCP Pools**: List of IPv6 DHCP pools.
	  • **DHCP Pool Name**: Name of the DHCPv6 pool.
	  • **DNS Server**: List of DNS server IPv6 addresses for DHCPv6 clients. Specify one or more DNS servers to be provided to clients for IPv6 name resolution.
	  • **DNS Default Domain Name**: List of domain names assigned to DHCPv6 clients.
	• **Excluded Addresses**: List of excluded addresses for DHCP.
	  • **Excluded Address Low**: Lowest IP address in the exclusion range for DHCP assignment. This marks the start of a block of addresses that will not be assigned by DHCP.
	  • **Excluded Address High**: Highest IP address to exclude from DHCP assignment. Use this to define the upper end of an exclusion range for reserved addresses.
	• **Excluded Low Addresseses**: In this tab, **Excluded Address Low** indicates the lowest IP address to exclude from DHCP assignment. Use this to reserve addresses that should not be assigned to clients.
	Note

Name	Description
	When adding a DHCP pool option, only supported option codes can be included.

Name	Description
AAA	

Name	Description

	View AAA settings to manage security by authenticating user identities, authorizing their access levels, and accounting for their network activity.
	• **AAA 802.1X Default Authentication**: Specifies the primary authentication servers used for network access control.
	• **Authorization Executive**
	  • **Method List Name**: Name of the AAA authorization method list for executive sessions.
	  • **Primary Server Group**: The first AAA server group for executive authorization.
	  • **Enable Primary Autherization After Authentication**: Enable or disable to grant access based on successful authentication.
	  • **Enable Primary Local Authorization**: Enable or disable to authorize users based on local credentials.
	  • **Secondary Server Group**: The second AAA server group for executive authorization.
	• **RADIUS Dynamic Authorizations (CoA)**
	  • **Client IP Address**: IP address of a RADIUS Dynamic Authorization (CoA) client for change of authorization.
	  • **Client Key Type**: Type of key used for RADIUS Dynamic Authorization client.
	• **AAA Identity Accounting Start-Stop**
	  • **Primary Server Group**: Tracks identity-related events for users and devices.
	  • **Secondary Server Group**: Used for backup or additional identity tracking.
	  • **Tertiary Server Group**: Provides more redundancy for identity accounting.
	  • **Quaternary Server Group**: Used for further backup or load balancing.
	• **Accounting Executive**
	  • **Method List Name**: First AAA server group for identity accounting with start-stop method.

Name	Description
	• **Primary Server Group**: Tracks user session starts and stops. • **Secondary Server Group**: A backup group for session accounting. • **Tertiary Server Group**: Additional redundancy for accounting and reliability. • **Quaternary Server Group**: Further backup or load balancing in accounting. • **RADIUS Global Config** • **Timeout Interval**: Time (seconds) to wait for a reply from a RADIUS server before a retry. • **Retransmit Count**: Number of retry attempts to the active RADIUS server before considering the request failed. • **Dead Time**: Duration (minutes) to stop using a RADIUS server that is not responding before marking it as dead. • **Dead Criteria Time**: Dead Criteria Time (seconds) determines how quickly the system switches to a backup server. • **Dead Criteria Tries**: Number of failed attempts before the device marks a RADIUS server as dead. • **RADIUS Servers** • **Server Name**: Identifier for the RADIUS server. • **Server IPv4 Address**: IPv4 address of the RADIUS server. • **Server IPv6 Address**: IPv6 address of the RADIUS server. • **Server Hostname**: Fully qualified domain name of the RADIUS server. • **Authentication Port**: Authentication port number for RADIUS server.

Name	Description
	• **RADIUS Server Group** • **Server Group Name**: Name of the RADIUS server group. • **Dead Time**: Dead time (minutes) for an unresponsive RADIUS server. • **Source Interface Loopback**: Loopback interface used as the source for Radius packets. • **IPv4 VRF Forwarding**: IPv4 VRF forwarding table for the RADIUS server group. • **IPv6 VRF Forwarding**: IPv6 VRF forwarding table for the RADIUS server group. • **TACACS+ Servers** • **Server Name**: Name of the TACACS+ server. • **IPv4 Address**: IPv4 address of the TACACS+ server. • **IPv6 Address**: IPv6 address of the TACACS+ server. • **Server Host Name**: Fully qualified domain name of the TACACS+ server. • **TCP Port**: TCP port number for the TACACS+ server. • **TACACS+ Server Group** • **Server Group Name**: Name of the TACACS+ server group for AAA operations. • **IPv4 VRF**: IPv4 VRF forwarding table for the TACACS+ server group.

Step 5 Click the **Edit** icon to update the configurations.

Note You cannot edit configurations for devices that are part of a network, device group, or Cisco SD-Access fabric network.

Step 6 Click **Next** after you edit the required configurations.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

View and edit service configurations of a device

Use this procedure to view and manage the service configurations.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name, then select **View Device Details**.

Step 3 Click **Configuration** and expand **Services**.

Step 4 Select **QoS**.

Step 5 Refer to the table to view and modify configuration details.

Table 15: QoS configuration details

Name	Description
Class Map	Displays a list of class maps with details. Class maps define the criteria used to match and classify specific network traffic flows. • **Class Map Name**: Name for the class map. • **Prematch**: Indicates the pre-match criteria for the class map. • **Description**: Description of the class map. • **Group Name**: The access list name. • **DSCP**: The DSCP match criteria for IPv4 and IPv6 packets.

Name	Description
Policy Map	Displays a list of policy maps. A policy map is a set of rules that define QoS actions applied to traffic. • **Policy Map Name**: Name of the policy map. • **Policy Map Description**: A description of the policy map. • **Policy Map Type**: The category or type of the policy map. • **Policy Map Subscriber**: The subscriber associated with the policy map.
Table Map	Displays a list of table maps. Table maps provide a way to map QoS marking values between different priority schemes. • **Table Map Name**: A name for the table map. • **Default Value**: Specifies value to be assigned when there is no matching map entry. • **Table Map Entries**: Specifies the source and destination markings.
Attribute To Service	Defines how specific traffic attributes are associated with QoS policy. A list of **Service Name**s is displayed.
Web Authentication	Defines QoS settings for web authentication. • **Web Authentication Name**: Name for the web authentication configuration. • **Web Authentication Type**: The type or method of web authentication being used.

Step 6 Click the **Edit** to update the configurations.

Step 7 Click **Next** to continue after editing the required configurations.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

View and edit industrial configuration of a device

Use this procedure to view and edit the industrial configurations of an Cisco Catalyst Industrial Ethernet (IE) Switches running Cisco IOS XE Release 26.1 and later.

Before you begin

You must enable per-device configuration to manage switch configurations. In the **Configuration** window, click **Learn more** and complete the steps to enable per-device configuration on the device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Devices** table, click the device name, and then click **View Device Details**.

Device details appear. The **Industrial** area displays a summary of the industrial configurations for your device.

Step 3 Use one of these options to view the industrial configuration details.

- In the **Industrial** configuration area, click **View Industrial Configuration Details**.
- Click the **Configuration** tab and expand **Industrial**.

Step 4 Refer to the table to view and modify configuration details.

Name	Description
CIP	View Common Industrial Protocol (CIP) details. • **Security Password**: The CIP security password. Password length must be between 1 and 32 characters. • **Window Timeout**: After the timeout duration, the CIP session shuts down. The valid range is 1 to 3600 seconds, and the default value is 600 seconds. • **Encap Inactivity Timeout**: Switches under CIP share the session timeout. The valid range is 0 to 3600 seconds. The default value is 120 seconds.
PROFINET	View these Profinet details: • **Enable Profinet**: View Profinet status—enabled or disabled. Enabled by default. • **Profinet VLAN ID**: The VLAN for the Profinet. The default VLAN ID is 1. • **Enable MRP**: View MRP status—enabled or disabled. Enabled by default.

Name	Description
Modbus	View the Modbus configuration details. • **Number of TCP connections**: View the number of parallel TCP connections supported. The valid range is 1 to 5. Default value is 1. • **Port Number**: TCP port number. The valid range is 1 to 65535. The default value is 502. • **Modbus Status**: View Modbus status on the device—enabled or disabled. Disabled by default.

Alarm	View the alarm settings for the device.
	• **Alarm Facility**: View the alarm facilities supported on the device. The device model determines the supported alarm facilities.
	  • Use **Edit** to modify the alarm facility configurations.
	• **Alarm Contact**: View the alarm contacts supported on the device.
	  • Click the number to view the contact details.
	  • Use **Edit** to modify the configuration.
	• **Alarm Profile**: View the alarm profiles supported on the device.
	  • Click the profile name to view the profile details.
	  • Use **Edit** to modify the configuration.

L2 NAT	View the Layer 2 Network Address Translation (L2 NAT) instances, including the fixup and permit type for each L2 NAT instance. Click the instance name to view the translation settings.

Step 5 Click **Edit** to add or update the configurations.

Step 6 Click **Next** after you edit the required configurations.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

View and edit port configuration of a device

Use this procedure to view and manage the port configurations.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name, then select **View Device Details**.

Step 3 Click **Configuration** and expand **Port**.

You can also view and manage the port details under the **Summary** tab. Refer to Manage port details, on page 94.

Step 4 Refer to the table to view and modify configuration details.

Table 16: Port configuration details

Name	Description
Port Channel	Displays the list of supported port channels including these details: • **Portchannel Number**: Identifier for the port channel interface. • **Description**: Text description of the interface. • **Admin Status**: Option to enable to disable the port channel interface. • **Layer 3**: Option to enable or disable the switchport mode on the interface. **Trunk Allowed VLANs**: List of allowed VLANs on the trunk for the port channel interface. Click on the port channel name to view details. Follow these steps to add a port channel: **a.** Click **Edit**. **b.** Click **Add**. **c.** In the **Add Port Channel** window, enter a **Portchannel Number** and configure other fields as needed. **d.** Click **Save**.

Name	Description
Ethernet Port	Displays the list of Ethernet ports configured on the device including these details: • **Port Name**: Ethernet port name. • **Layer 3**: Option to enable or disable the switchport mode on the interface. • **Description**: Text description for the port. • **Admin Status**: Option to enable to disable the interface. • **Trunk Allowed VLANs**: List of allowed VLANs on the trunk for the interface.

Step 5 Click the **Edit** icon to update the configurations.

Step 6 Click **Next** after you edit the required configurations.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Inventory user interface enhancement

The enhanced Catalyst Center inventory user interface provides the existing inventory features. It also includes improved filters and an updated layout for a better user experience.

Before you begin

Make sure that you have devices in your inventory; otherwise, use the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The enhanced **Inventory** window appears by default and displays the device information gathered during the discovery process.

Step 2 Click the location option in the top menu bar. Then select the site, building, or floor from the network hierarchy to manage your device.

Step 3 Use the device families area at the top of the **Inventory** window to select one or more device families.

The available device families include **Routers**, **Switches**, **Wireless Controllers**, **Access Points**, and **Sensors**.

Step 4 Use the **Focus** drop-down list to filter the devices based on **Inventory**, **Default**, **Software Image**, **Provision**, **Security**, or **Device Replacement**.

Step 5 Use the divider bar at the left corner of the **Device** table to collapse or expand the table width.

Step 6 In the **DEVICE WORK ITEMS** area, select one or more filter criteria to narrow down the devices in the table.

Step 7 Click **Add Device** to add a new device to the inventory. For more information, see Add devices to the Catalyst Center Inventory, on page 128.

Step 8 Use **Tag** to tag a device. For more information, see Manage devices in the Inventory window, on page 156.

Step 9 Use the **Action** drop-down list to perform actions on one or more devices.

Step 10 Click the **i** icon to learn about the list of actions and their respective functionalities.

Step 11 To edit or customize the inventory table, click the gear icon in the right corner at the top of the table and do these steps:

a. Click **Table Appearance** to define the **Table Density** and **Table Striping**.

b. Click **Edit Table Columns** to select the device information that you want to include in the inventory table during the discovery process.

c. Click **Edit Custom Views** to customize your current view.

d. Click **Apply** to save the changes or click **Reset All Settings** to apply the default settings for the inventory table.

Step 12 Use the **Filter Devices** option to apply the advanced filter in your device table. For more information, see Filter Devices.

Step 13 Click the toggle buttons at the top-right corner to switch between **Dashboard**, **Table**, **Topology**, and **Map** view.

Step 14 Click **Go to old page** to navigate to old inventory window.

Step 15 Use **Export** to export all data in the device table.

Manage user-defined fields

User-defined fields are custom labels. You can create and assign these labels to any device in Catalyst Center. These labels allow you to display more details about the device. Assign a user-defined field to a device and add a value to display more details.

Create user-defined fields

Catalyst Center allows you to create user-defined fields and assign them to any device.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 In the **Devices** table, click the name of a device, and then click **View Device Details**.

Step 3 Click **Details** and then **User Defined Fields**.

Step 4 Click **Manage user defined fields**.

Step 5 Click **Create new field**.

Step 6 In the **Create new field** dialog box, enter a field name and description.

Note You can add device details that are not already present in the **Device Details** window, such as customer IP address and customer device name.

Step 7 Click **Save**.

To create more user-defined fields, click **Create new field** again.

Step 8 (Optional) To edit a user-defined field, click **Edit**, make the required changes, and click **Save**.

Step 9 (Optional) To delete a user-defined field, click **Delete** and confirm.

Add user-defined fields to a device

Before you begin

You must have created at least one user-defined field in the **Manage User Defined Fields** window. For more information, see Create user-defined fields, on page 126.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

Step 2 Click the name of the device for which you want to add user-defined fields, and then click **View Device Details**.

Step 3 In the left pane, click **User Defined Fields**.

Step 4 Click **Add User Defined field**.

Step 5 From the **Field Name** drop-down list, choose a user-defined field and enter its value in the **Value** field.

For example, if you created a user-defined field for the customer IP address, choose it from the **Field Name** drop-down list, and enter the customer IP address in the **Value** field.

Step 6 (Optional) To remove a user-defined field from the device, click the corresponding delete icon.

Step 7 Click **Save**.

Launch Topology map from Inventory

You can launch the Topology map for the discovered devices from the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Use the toggle button ( ) to switch between the Topology map view and the Inventory view. The Topology map view displays the topology and the provisioning status of the device. Click each node to view the device details. For more information about the Topology map, see About topology, on page 219.

Note Click **Collapse All** or **Expand All** to collapse and expand the Topology map view.

Types of devices in the Catalyst Center Inventory

Devices appear in the inventory in one of two ways: through discovery or by manual addition. Catalyst Center Inventory supports various types of devices, including:

- **Network Devices**: Supported network devices include Cisco routers, switches, and wireless devices such as wireless controllers and access points (APs).
- **Compute Devices**: Supported compute devices include the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.
- **Meraki Dashboard**: Dashboard to the Cisco cloud management platform for managing Cisco Meraki products.
- **Firepower Management Center (FMC)**: Provides complete and unified management over Firepower Threat Defense (FTD) devices for managing Cisco network security solutions.
- **Third-Party Devices**: Third-party devices are capable of populating SNMP MIB 2 values. Catalyst Center supports limited base automation for inventory and topology. Additionally, assurance capabilities cover third-party device 360, device health calculation based on reachability status, as well as device interface and reachability issues.

For a complete list of supported devices, see the *Cisco Catalyst Center Compatibility Matrix*.

Add devices to the Catalyst Center Inventory

You can add both new and existing devices to the Catalyst Center Inventory.

When adding or managing devices, note these constraints regarding dual-stack IP address families (IPv4 and IPv6):

- Conflict prevention: You can't add the same device using both IPv4 and IPv6.
- FQDN handling:

- FQDNs must be resolvable in a dual-stack environment. If an FQDN can't be resolved or lacks a valid DNS record, the device addition fails.
- Devices added via FQDN are automatically assigned an address family (IPv4 or IPv6) based on the successful DNS resolution result.

- After a device is added, you can't change its address family. To switch a device from IPv4 to IPv6 (or vice versa), you must remove the device from the inventory and re-add it using the desired IP type.
- If an IP type conflict is detected during inventory collection, the system halts updates for that device and marks it as "Error" to prevent data inconsistency.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Click **Add Device**.

The **Add Device** slide-in pane provides options for adding new devices using Plug and Play or adding existing devices.

Step 3 Select an option to add existing devices to your inventory.

- To add devices using the discovery process, click **Discovery** and follow the workflow. For more information, see Discover devices, on page 1374.
- To add a single device, click **Single Device**. Choose the type of device that you want to add.
  - To add a network device, see Add a network device, on page 130.
  - To add a compute device, see Add a compute device, on page 141.
  - To integrate the Meraki dashboard, see Integrate the Meraki dashboard, on page 148.
  - To integrate the Firepower Management Center, see Integrate Firepower Management Center, on page 149.
  - To add a third-party device, see Add a third-party device, on page 151.
- To import device configuration from a CSV file, click **Import Inventory**. For more information, see Import device configurations from a CSV file, on page 186.

Step 4 Select an option to add existing devices to your inventory.

New devices are added using the Plug and Play process. You can add a single device, multiple devices, or devices from a Smart Account. Selecting any tile opens the options in the **Plug and Play** window.

- To add a single device, click **Single Device**. For more information, see Add or edit a device, on page 596.
- To add devices in bulk from a CSV file, click **Bulk Devices**. For more information, see Add devices in bulk, on page 597.

- To add devices from a Smart Account, click **Smart Account**. For more information, see Add devices from a Smart Account, on page 599.

What to do next

You can view and manage the devices in your inventory. For more information, see Manage devices in the Inventory window, on page 156. To manage the newly added devices from the **Plug and Play** window, see View devices, on page 594.

Manage network devices

Add a network device

You can add a network device to your inventory manually.

Before you begin

Make sure you configure your network device. For more information, see Discovery prerequisites, on page 56.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The discovery process gathers the device information, which is then displayed in the **Inventory** window.

Step 2 Click **Add Device**.

The **Add Device** slide-in pane appears with options to add devices.

Step 3 In the **Existing devices** area, click the **Single Device** tile.

Step 4 From the **Device type** drop-down list, choose **Network Device**.

Step 5 In the **IP address** field, enter the IP address or name of the device.

Note If the device uses the HSRP protocol, you must enter the primary IP address.

Step 6 Configure the **CLI** credentials.

a) To use global credentials, click the global credential radio button.

Note If no CLI global credentials are available, create the global CLI credentials in the **Network Settings** > **Device Credentials** window. See Add global CLI credentials, on page 323.

b) To configure credentials for the specific device, click **Add** and configure these fields:

Table 17: CLI credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials. If authentication fails for CLI, Catalyst Center retries the authentication process for 300 seconds (5 minutes).
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Step 7 Configure the **SNMP** credentials.

a) To use global credentials, click the global credential radio button.

Note If no SNMP global credentials are available, create the global SNMP credentials in the **Network Settings** > **Device Credentials** window. See Add global SNMPv2c credentials, on page 324 and Add global SNMPv3 credentials, on page 325.

b) To configure credentials for the specific device, click **Add** and then continue this procedure.

Step 8 From the drop-down list, choose **SNMPv2C** or **SNMPv3**.

If you select SNMPv2c, configure these fields:

Table 18: SNMPv2c credentials

Field	Description
Name/Description	Name or description of the SNMPv2c settings that you are adding.
Read Community	Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

Field	Description
Write Community	Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

If you choose SNMPv3, configure these fields:

Table 19: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Select one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Select one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Select one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.

Step 9 Configure the **NETCONF** settings.

Note NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Table 20: NETCONF setting

Field	Description
Port	Port on the device. You can use one of these ports: • Port 830 (default). • Any other port that is available on the device. • A custom port that Catalyst Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.) If authentication fails for NETCONF, Catalyst Center retries the authentication process for 300 seconds (5 minutes).

Step 10 Click **Show advanced settings** and configure the required settings as described in the next steps.

Step 11 Configure the **Retries** and **Timeout** value for SNMP.

Table 21: SNMP properties

Field	Description
Retries	Number of times Catalyst Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

Step 12 Configure the **HTTP(S)** credentials.

a) Click the global credential radio button to use the global HTTP(S) credentials that have already been created.

Note If no HTTP or HTTPS global credentials are available, create the global HTTP or HTTPS credentials in the **Network Settings** > **Device Credentials** window. See Configure Global HTTP(S) Credentials.

b) To configure credentials for the specific device, click **Add** and configure these fields:

Table 22: HTTP and HTTPS credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Field	Description
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Step 13 Select one of the network **Protocol** that enables Catalyst Center to communicate with remote devices. Valid values are **SSH2**, or **Telnet**.

Step 14 (Optional) Click **Validate** next to **Credentials**. Catalyst Center validates the device credentials. A green tick mark indicates valid credentials. A red cross mark indicates invalid credentials.

The process validates all credentials except the SNMP Write credentials.

Step 15 Review the configurations. (Click **Edit** to make any changes.)

Step 16 Click **Add Device**.

Update network device credentials

You can update the discovery credentials of selected network devices. The updated settings override the global and job-specific settings for the selected devices.

Note You cannot update the credentials of a third-party device that is added to the inventory.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to do this procedure.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Select the network devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 Expand the **CLI** area, if it is not already expanded, and do one of these steps:

a) If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.



Note If no CLI global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Configure Global CLI Credentials.

b) Click the **Add device specific credential** radio button and configure these fields:

Table 23: CLI credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. To confirm the password for security reasons, re-enter it. Passwords are encrypted for security reasons and do not display in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. To confirm the password for security reasons, re-enter it. Passwords are encrypted for security reasons and do not display in the configuration.

Step 5 Expand the **SNMP** area, if it is not already expanded, and do one of these steps:

a) If you want to use the global SNMP credentials that have been already created, click the **Select global credential** radio button.



Note If no SNMP global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Configure Global SNMPv2c Credentials and Configure Global SNMPv3 Credentials.

b) Click the **Add device specific credential** radio button then continue with this procedure.

Step 6 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure these fields:

Table 24: SNMPv2c credentials

Field	Description
Read Community	Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.
Write Community	Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

If you select **V3**, configure these fields:

Table 25: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Select one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Select one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.

Field	Description
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Select one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.

Step 7 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure these fields.

Table 26: SNMP properties

Field	Description
Retries	Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
Timeout	Number of seconds Catalyst Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

Step 8 Expand the **HTTP(S)** area, if it is not already expanded, and do one of these steps:

a) If you want to use the global HTTP and HTTPS credentials that have already been created, click the **Select global credential** radio button.

Note If no HTTP or HTTPS global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Configure Global HTTP(S) Credentials.

b) Click the **Add device specific credential** radio button and configure these fields:

Table 27: HTTP and HTTPS

Field	Description
Username	Name that is used to log in to the HTTP and HTTPS of the devices in your network.
Password	Password that is used to log in to the HTTP and HTTPS of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are hidden in the configuration.
Port	Specify the required HTTP or HTTPS port number.

Step 9 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 10 Select one of the network **Protocol** radio buttons that enables Catalyst Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.

Step 11 (Optional) Click **Validate** next to **Credentials**. Catalyst Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button disables.

Step 12 Click **Update**.

Security focus for network devices

The Catalyst Center security focus allows you to view the results of the trustworthy checks on your devices.

Few security checks are done to ensure that your Cisco devices are authentic and are not compromised or altered physically.

As a part of device identity verification, checks run, including:

- Verification of Secure Unique Device Identifier (SUDI) certificate chain.
- Signature verification of SUDI certificate response of the device.
- Product ID verification with the SUDI certificate.
- Serial number verification with the SUDI certificate.

These checks are triggered under these circumstances:

- Every time Inventory gets collected in the Catalyst Center.

- When you make any configuration changes on your devices.
- When you make any image upgrades in your devices.

This CLI command is used to do a device identity verification check:

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

View the integrity verification status of a device

This procedure explains how to view the status of the integrity verification check.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 From the **Focus** drop-down menu, choose **Security**.

Step 3 In the **Devices** table, if the **Integrity Verification** column for your device displays **Failed** as the status, click the information icon (ⓘ) to display the reason.

Note If the **Integrity Verification** column is not displayed, see Display information about your inventory, on page 80.

View device certificate status

Device certificates are the certificates that are issued by Catalyst Center to authenticate the devices managed by it.

Use this procedure to view the device certificate status.

Note You can view the number of device certificates that are expiring or expired on the **Device Certificate Issues** tile, on Catalyst Center home window.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The Inventory window displays the device information that is gathered during the discovery process.

Step 2 From the **Focus** drop-down list, choose **Security**.

Step 3 You can view the device certificate status under **Certificate Status** column.

One of these statuses display:

Item	Description
Active	Certificate is valid.
Expiring	Check SCEP connectivity or configuration required for device to renew the certificate.
Expired	If this is unexpected, you can generate a new certificate for the device using the instructions in this Update device configuration using telemetry, on page 50.
Not Provisioned	Certificate is not provisioned.
NA	Device certificate status is yet to be available. Please check again later.

Step 4 To view the device certificate details, click the device certificate status hyperlink.

Manage compute devices

Add a compute device

You can add a compute device to your inventory manually. A compute device includes devices such as the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Click **Add Device**.

The **Add Device** slide-in pane appears with options to add devices.

Step 3 In the **Existing devices** area, click the **Single Device** tile.

Step 4 From the **Device type** drop-down list, choose **Compute Device**.

Step 5 In the **IP address** field, enter the IP address or name of the device.

Step 6 Configure the **HTTP(S)** credentials.

a) If you want to use the global HTTP or HTTPS credentials that have already been created, click the global credential radio button.

Note If no HTTP or HTTPS global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Add global HTTPS credentials, on page 327.

b) To configure credentials for the specific device, click **Add** and configure these fields:

Table 28: HTTP and HTTPS

Field	Description
Name or description	Name or description for the credentials.
Username	Name used to authenticate the HTTPS connection.
Password	Password used to authenticate the HTTPS connection.
Port	Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

Step 7 Click **Show advanced settings** and configure the required settings as described in the next steps.

Step 8 Configure the **CLI** credentials.

a) If you want to use the global CLI credentials that have been already created, click the global credential radio button.

Note If no CLI global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Add global CLI credentials, on page 323.

b) To configure credentials for the specific device, click **Add** and configure these fields:

Table 29: CLI credentials

Field	Description
Name or description	Name or description for the credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. For security reasons, re-enter the enable password. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 9 Configure the **SNMP** credentials.

a) If you want to use the global SNMP credentials that have been already created, click the global credential radio button.

Note If no SNMP global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Add global SNMPv2c credentials, on page 324 and Add global SNMPv3 credentials, on page 325.

b) To configure credentials for the specific device, click **Add** and configure these fields:

Step 10 From the drop-down list, choose **SNMPv2C** or **SNMPv3**.

If you select SNMPv2c, configure these fields:

Table 30: SNMPv2c credentials

Field	Description
Name/Description	Name or description of the SNMPv2c settings that you are adding.
Read Community	Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.
Write Community	Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

If you choose SNMPv3, configure these fields:

Table 31: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Select one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.

Field	Description
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Select one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Select one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.

Step 11 (Optional) Click **Validate** next to **Credentials**. Catalyst Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.

All the credentials will be validated except the SNMP Write credentials.

Step 12 Review the configurations. (Click **Edit** to make any changes.)

Step 13 Click **Add Device**.

Update compute device credentials

You can update the discovery credentials of selected compute devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 Expand the **HTTP(S)** area, if it is not already expanded, and do one of these steps:

a) If you want to use the global HTTP and HTTPS credentials that have already been created, click the **Select global credential** radio button.

Note If no HTTP or HTTPS global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Add global HTTPS credentials, on page 327.

b) Click the **Add device specific credential** radio button and configure these fields:

Table 32: HTTP and HTTPS

Field	Description
Username	Name that is used to log in to the HTTP and HTTPS of the devices in your network.
Password	Password that is used to log in to the HTTP and HTTPS of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are hidden in the configuration.
Port	Specify the required HTTP or HTTPS port number.

Step 5 Expand the **CLI** area, if it is not already expanded, and do one of these steps:

a) If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.

Note If no CLI global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Add global CLI credentials, on page 323.

b) Click the **Add device specific credential** radio button and configure these fields:

Table 33: CLI credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. To confirm the password for security reasons, re-enter it. Passwords are encrypted for security reasons and do not display in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. To confirm the password for security reasons, re-enter it. Passwords are encrypted for security reasons and do not display in the configuration.

Step 6 Expand the **SNMP** area, if it is not already expanded, and do one of these steps:

a) If you want to use the global SNMP credentials that have been already created, click the **Select global credential** radio button.

Note If no SNMP global credentials are available, create them in the **Network Settings** > **Device Credentials** window. See Add global SNMPv2c credentials, on page 324 and Add global SNMPv3 credentials, on page 325.

b) Click the **Add device specific credential** radio button then continue with this procedure.

Step 7 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure these fields:

Table 34: SNMPv2c credentials

Field	Description
Read Community	Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.
Write Community	Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

If you select **V3**, configure these fields:

Table 35: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Select one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Select one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Select one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are hidden in the configuration.

Step 8 (Optional) Click **Validate** next to **Credentials**. Catalyst Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Meraki dashboards

Integrate the Meraki dashboard

You can integrate your Meraki dashboard with Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Click **Add Device**.

The **Add Device** slide-in pane appears with options to add devices.

Step 3 In the **Existing devices** area, click the **Single Device** tile.

Step 4 From the **Device type** drop-down list, choose **Meraki Dashboard**.

Step 5 Configure the **HTTP(S)** credentials.

a) In the **API Key/Password** field, enter the API key used to access the Meraki dashboard. Then, click the **Get Organization details** link.

b) From the **Select Meraki Details** drop-down list, select the organization options, or search for an organization name.

Step 6 (Optional) Click **Validate** next to **Credentials**. Catalyst Center validates the device credentials, indicating valid credentials with a green tick mark and invalid credentials with a red cross mark.

Step 7 Review the configurations. (Click **Edit** to make any changes.)

Step 8 Click **Add Device**.

Only the selected organizations start collecting for the Meraki dashboard and devices.

Update Meraki dashboard credentials

You can update the Meraki dashboard credentials of selected devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 Expand the **HTTP(S)** area, if it is not already expanded.

Step 5 In the **API Key / Password** field, enter the API key used to access the Meraki dashboard.

Step 6 Click **Get Organization details**.

Step 7 From the **select meraki details** drop-down list, select the organization options, or search for an organization name.

Step 8 (Optional) Click **Validate** next to **Credentials**. Catalyst Center validates the device credentials, indicating valid credentials with a green tick mark and invalid credentials with a red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Firepower Management Center

Integrate Firepower Management Center

You can integrate your Firepower Management Center (FMC) with Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Click **Add Device**.

The **Add Device** slide-in pane appears with options to add devices.

Step 3 In the **Existing devices** area, click the **Single Device** tile.

Step 4 From the **Device type** drop-down list, select **Firepower Management Center**.

Step 5 In the **IP address** field, enter the IP address or name of the device.

Step 6 Configure the **HTTP(S)** credentials.

a) **Username**: Name used to authenticate the HTTPS connection.

b) **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not visible in the configuration.

c) **Port**: The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.

Step 7 Review the configurations. (Click **Edit** to make any changes.)

Step 8 Click **Add Device**.

Note When you add FMC to inventory, the Firepower Threat Defense (FTD) devices managed by FMC are also added to inventory automatically. The **Inventory** window displays the available High Availability (HA) pairs, including details of active and standby FTDs.

Step 9 To view the HA details of the paired FTDs:

a) Click the device name of FTD.

b) Click **View Device Details**.

The paired FTD name is shown in the **Device Details** window. You can click the paired FTD name to view the paired FTD details.

c) In the **Device Details** window, click **High Availability Details**.

You can view the **HA Pair Info**, **High Availability Link**, and **State Link** details.

Update Firepower Management Center credentials

Catalyst Center allows you to update the Firepower Management Center (FMC) credentials. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Choose the FMC device that you want to update.

Note You cannot update, edit, or delete the Firepower Threat Defense (FTD) devices that are managed by FMC. You must manage FTD devices though FMC in inventory.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** slide-in pane, click **Credentials**.

Step 5 Expand the HTTP(S) area if it is not already expanded.

The **Add device specific credential** radio button is chosen by default.

Step 6 Enter this information:

a) **Username**: Name used to authenticate the HTTPS connection.

b) **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.
c) **Port**: The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.

Step 7 Click **Management IP** and enter the IP address or name of the device in the **Device IP / DNS Name** field.

Step 8 Click **Resync Interval** and choose a resync interval type:

- **Custom**: You can enter the resync interval in minutes. The valid range is from 360 to 1440 minutes (24 hours).
- **Global**: By default, resync interval is set to 1440 minutes (24 hours).
- **Disable**: Resync interval is disabled or set to zero.

Step 9 Click **Role** and choose a role in the **Device Role** drop-down list.

Step 10 Click **Update**.

Add a third-party device

You can add a third-party device to your inventory manually.

Catalyst Center supports limited base automation (Inventory and Topology) and assurance capabilities, such as third-party device 360, device health calculation based on reachability status, and device interface and reachability issues.

For third-party devices, reachability and interface-related metrics are captured as part of Assurance capabilities. For more information, refer to *Cisco Catalyst Assurance User Guide*.

Some of the third-party devices are capable of populating SNMP MIB-II values. For more information, refer to the *Cisco Catalyst Center Compatibility Matrix*.

Before you begin

Make sure you configure your network device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information.

Step 2 Click **Add Device**.

The **Add Device** slide-in pane displays.

Step 3 To add a device to your network, click the **Single Device** tile in the **Existing devices** area and do these steps:

a) Choose **Third Party Device** from the **Device type** drop-down list.
b) In the **IP address** field, enter the IP address or unique name for the device.
c) (Optional) Click the **Validate** hyperlink in the **Credentials** area to validate the device credentials. A green tick mark appears for valid credentials. A red cross mark appears for invalid credentials.

Note All the credentials are validated except the SNMP Write credentials.

d) Configure the **SNMP** credentials.

1. To use global SNMP credentials, choose the global credential radio button and click the **Network Settings** > **Device Credentials** hyperlink to add the credentials. For more information, refer to Add global SNMPv2c credentials, on page 324 and Add global SNMPv3 credentials, on page 325.
2. To configure credentials for the specific device, click **Add** and configure these fields:
   a. From the drop-down list, choose **SNMPv2C** or **SNMPv3**.
   b. If you select SNMPv2c, configure these fields:

Table 36: SNMPv2c credentials

Field	Description
Name/Description	Name or description of the SNMPv2c settings that you are adding.
Read Community	Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.
Write Community	Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are hidden in the configuration.

   c. If you choose SNMPv3, configure these fields:

Table 37: SNMPv3 credentials

Field	Description
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.

Field	Description
Authentication Type	Authentication type to be used (enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**). Choose one of these authentication types: • **SHA**: Authentication based on HMAC-SHA. • **SHA256**: Authentication based on HMAC-SHA256. • **MD5 (not recommended)**: Authentication based on HMAC-MD5. **Note** Catalyst Center does not support device discovery if only MD5 authentication type is configured on the device for software image version 17.14.1 and later. To use MD5 authentication, also configure SHA authentication. This configuration enables Catalyst Center to discover and manage devices running on software image 17.14.1 and later.
Authentication Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type (enabled if you select **Authentication and Privacy** as **Mode**). Choose a privacy type. **AES128**: 128-bit CBC mode AES for encryption. **Note** Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and do not display in the configuration.

e) Click **Show advanced settings** and configure the required settings as described in the next steps.
f) Configure the **Retries** and **Timeout** value for SNMP.

Table 38: SNMP properties

Field	Description
Retries	Number of times Catalyst Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Time interval between the retries.

Step 4 Review the configurations. (Click **Edit** to make any changes.)
Step 5 Click **Add Device**.

Filter devices

In the **Inventory** window, you can choose from basic or advanced options to filter for device details in the **Devices** table.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Click **Filter devices**.

This table describes the available filtering options.

Name	Description
Quick Filters	You can choose from basic filtering options to narrow down the device details. For example, you can toggle the **Manageability** filter option to **Managed** to see all the managed devices.
Advanced Filters	You can set the filtering criteria using operators, such as **Contains** and **Regex** (Regular Expression), to narrow down the device details. For example, in the **Tags** drop-down list, you can choose the **Contains** operator and enter **`ipsec`** in the **Tags** field. Then from the autocomplete drop-down list, you can choose one option, such as **branch-router-ipsec**, which would filter for branch routers that are tagged with IP Security. You must enter filter criteria values based on the available data.
Recent Filters	In the **RECENT** area, you can choose a recent filter to reapply. To save a recent filter, drag and drop a recent filter to the **SAVED** area.

Step 3 Choose a filtering option and enter the appropriate value in the selected filter field.

Catalyst Center presents you with autocomplete values as you enter values in the other fields. Choose one of the suggested values, or finish entering the desired value.

For complex wildcard filtering scenarios, use the regex option under **Advanced Filtering**. These examples show how to use regex filtering with wildcards:

Regex with Wildcards	Result
^AP00.*9.*	Filters device names that start with AP00 and contain 9 anywhere in the remainder of the device name.
^AP84.*24.*	Filters device names that start with AP84 and contain 24 anywhere in the remainder of the device name.
^.*47B3.*24.*	Filters device names that contain 47B3 and also contain 24 anywhere in the remainder of the device name.

After entering the regex values, press **`Enter`**.

Step 4 Click **Apply** to filter the information.

The data displayed in the **Devices** table updates automatically according to your filter selection.

Note You can use several filter types and more than one value per filter.

Step 5 (Optional) If needed, add more filters.

Step 6 (Optional) To remove all the filters, in the **Filter devices** field, click the **x** and then click **Apply**.

Step 7 (Optional) To delete a specific filter value, in the **Filter devices** field, drag your cursor over the value, press **`Delete`**, and then click **Apply**.

Manage devices in the Inventory window

These sections provide information about how to assign devices to sites and manage device tags by using the **Inventory** window.

Assign an unprovisioned device to a site

Use this procedure to assign a device that hasn't been provisioned yet to a site.

Note

- A wireless AP that hasn't been provisioned yet can be assigned to only a floor. Later, if it's still unprovisioned, it can be unassigned from the floor by removing it from its assigned floor map. For detailed steps, see Remove APs from a map, on page 275.
- Third-party devices can be assigned to a site, but the devices are not managed by Catalyst Center. It's only for visibility.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box for the devices that you want to assign to a site.

Note You cannot assign Firepower Threat Defense (FTD) high availability (HA) paired devices to different sites. Assign both devices in the pair to the same site.

Step 3 From the **Actions** menu, choose **Provision** > **Assign Device to Site**.

Step 4 In the **Assign Device to Site** slide-in pane, click the link next to the Site icon ( ) for the device.

Step 5 In the **Choose a floor** slide-in pane, select the floor to assign to the device and click **Save**.

Step 6 (Optional) If you select multiple devices to add to the same location, check the **Apply to All** check box for the first device to assign its location to the rest of the devices and click **Next**.

Step 7 Review summary settings and click **Next**.

Note Application Telemetry and Controller-Based Application Recognition (CBAR) is enabled on the applicable network devices by default, if you enable **Application Telemetry** and **CBAR** in the **Design** > **Network Settings** > **Telemetry** window. For more information, see Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 43.

Application and Endpoint Visibility enablement is skipped by default for the devices that does not support Controller-Based Application Recognition (CBAR) enablement or undeployed Application Visibility Service (AVS).

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note If only MD5 authentication type is configured on the device, the site assignment will be blocked for devices with software image version or golden tagged image version 17.14.1 and later.

To continue the site assignment, you must configure SHA authentication as well. For information on how to configure SHA as the authentication type for SNMP credentials, see Edit Global Device Credentials.

Step 9 On the **Tasks** window, monitor the task deployment.

Step 10 When assigning devices to a site, if **Device Controllability** is enabled, a workflow automatically triggers to push the device configuration from the site to the devices.

For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.

From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled **Device Controllability**.

Assign a provisioned device to a different site

Follow these high-level steps to assign any provisioned device, except provisioned wireless APs, to a different site.

To assign a provisioned wireless AP to a different floor, you must choose a different site for the AP during AP reprovisioning. For more information about reprovisioning, see Provision Cisco APs on day 1, on page 627.

Procedure

Step 1 Delete the provisioned device that you want to reassign to a different site from the inventory.

For detailed steps, see Delete a network device, on page 183.

Step 2 Readd the device that you deleted back to the inventory.

For detailed steps, see Add a network device, on page 130.

Step 3 Assign the newly added device to the required site.

For detailed steps, see Assign an unprovisioned device to a site, on page 156.

Tag devices

A device tag allows you to group devices based on an attribute or a rule. Each device can have multiple tags, and each tag can apply to multiple devices.

When a device or port is tagged, it becomes a member of that tag. There are two types of tags:

- Static: You can manually assign these tags to members.
- Dynamic: Catalyst Center automatically assigns these tags to members based on the defined rules.

When a device is deleted and then re-added:

- Static tags aren't reassigned to the members.
- Dynamic tags are reassigned to members that meet the defined rules for the tag.

You can add or remove tags from devices in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box next to the devices for which you want to apply a tag, and then click **Tag**.

Step 3 Enter a tag name in the **Tag Name** field.

- To create a tag, click **Create New Tag**. You can also create a new tag with a rule. Refer to Tag devices using rules, on page 160.
- To use an existing tag, select the tag from the list, and then click **Apply**.

A tag icon and the tag names appear under the device names for which you applied the tags.

Step 4 To remove a tag from a device, do one of these tasks:

- Select the device and click **Tag**. Unselect all tags, and then click **Apply**.

- Click the yellow tag icon or tag name, then click the delete icon to remove the tag from the device.

Create a Network Device Group tag

Use this procedure to create a Network Device Group (NDG) tag.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays device information found during discovery.

Step 2 Check the check box next to the device for which you want to apply a tag, and then click **Tag**.

Step 3 Click **Create New Tag**.

For the naming pattern, use the prefix **NDG:**. Set the tag with the parent-child hierarchy. Use roots for all NDG types. For example, use Location#All Locations, Device Type#All Device Types, or IPsec#Is IPsec. Use the entire root while creating the NDG tags.

Note

- Custom roots are not allowed while creating the NDG tag. Only default NDG roots in Cisco ISE are allowed, which are Location#All Locations, Device Type#All Device Types, and IPSEC#Is IPSEC.

  Cisco ISE will always have default NDG roots for devices unless they are overridden by Catalyst Center NDG tags.
- Only one NDG tag can be added per NDG type for a device.
- The hierarchy can have up to seven levels, including parent and roots. Include at least one child level when you create tags.
- Each level name cannot exceed 32 characters. The tag length cannot exceed 100 characters.
- NDG tags support the standard ASCII character set.
- Catalyst Center doesn't reflect the NDG values set in Cisco ISE. A NDG tag update in Catalyst Center overrides the values set in Cisco ISE.

A tag icon and name appear under the device name for which you applied the tag.

Note Tags with the prefix **NDG:** are reflected in Cisco ISE.

Tag devices using rules

You can group devices by creating rules that define tags. When you define a rule, Catalyst Center automatically applies the tag to all devices that match the rule. You can base rules on device name, device family, device series, IP address, location, or version.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box next to each device you want to tag, then click **Tag**.

Step 3 Enter a tag name in the **Tag Name** field, then click **Create New Tag with Rule**.

In the **Create New Tag** window, the **Manually Added** field under **Total Devices Tagged Count** indicates the number of devices you selected.

Step 4 Click **Add Condition** and complete the required fields for the rule.

The **Matching Devices** number automatically changes to indicate how many devices match this condition.

You have two options to create additional conditions:

- *And* conditions: Click the **Add Condition** link. **And** appears above the condition.
- *Or* conditions: Click the add icon (plus sign) next to an existing condition. **Or** appears next to the condition.

You can add as many conditions as needed. As you change to the rule, the Matching Devices count updates to show how many devices match it. Click the device number to view matching devices.

Step 5 Click **Save** to save your tag with the defined rule.

A tag icon and the tag name appear below the device name for each device you tagged.

As devices are added to the inventory, if they match the rules you defined, the tag is automatically applied to the devices.

Edit device tags

You can edit device tags that you previously created.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window shows device information found during the discovery proces.

In the **Device Name** column, you can see any previously created device tags listed under the device names.

Step 2 Without selecting any devices, click **Tag**.

The previously created tags are listed.

Step 3 Click **Manage Tags**.

The **All Tags** slide-in pane appears.

Step 4 Click the pencil icon next to the tag you want to edit.

Step 5 Edit to the tag, then click **Save**.

Delete tags

You can delete a device tag or template tag only if it is not associated with a device or template.

Before you begin

Use rules to remove the tags associated statically or dynamically with the device.

Remove the tag that is associated with a template.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Without selecting any devices, choose **Tag** > **Manage Tags**.

Step 3 Hover your cursor over the tag that you want to delete, then click the delete icon next to the tag name.

Step 4 At the prompt, click **Yes**.

If the tag is associated with a device or template, an error message appears. Remove the tag that is associated with the device or template, and then delete the tag.

Deal with SSH key verification errors

In the **Inventory** window, Catalyst Center indicates the devices for which SSH key verification failed. To deal with this error, complete these steps.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Manageability** column, click the **SSH key verification failed** link for the device.

Step 3 In the dialog box that opens, follow one of these procedures:

If...	Then...
you want to enable or disable the automatic and global acceptance of SSH key changes,	click **SSH key configuration**. For more information, refer to Configure the automatic acceptance of SSH key changes, on page 162.
you want to open a slide-in pane that lists all devices with SSH key verification errors,	**a.** Click **All errors**. **b.** Check the check box for the devices with SSH key changes you approve. **c.** Click **Confirm**. This triggers a resync of the selected devices.
you know that the SSH key for a device was changed intentionally,	click **Confirm**. This triggers a resync of the device.

Configure the automatic acceptance of SSH key changes

In the **SSH key configuration** window, you can configure whether Catalyst Center automatically accepts SSH key changes.

Important When this option is enabled, you must manually resync every device on which SSH key verification failed.

Procedure

Step 1 From the main menu, choose **System** > **Device Settings** > **SSH key trust**.

Step 2 Click the **Accept all changes** toggle button to enable or disable the automatic acceptance of any SSH key changes that are made.

Configure a REP ring for devices

The Resilient Ethernet Protocol (REP) ring provides a way to control network loops, handle link failures, and improve convergence time.

Note

- Limitation of a REP ring: You should not select a root node that has connectivity only through interfaces of the ring.
- Device support for REP ring (nonfabric): Cisco Catalyst Industrial Ethernet (IE) Series Switches 3100, 3200, 3300, 3400, 4000, 5000, and 9300, as well as Cisco Embedded Services 3300 Series Switches (ESS3300), S5200, and S5800.
- You can configure REP ring with MACsec encryption.

  Cisco Catalyst IE 3100 Series switches and Cisco Catalyst 9000 Series switches do not support MACsec encryption with a REP ring.

Before you begin

- Make sure the devices are onboarded and are in reachable state.
- Identify the devices and their interfaces that end the REP ring.
- Make sure every interface in the ring is configured with “switchport mode trunk”.

Procedure

Step 1 From the main menu, choose **Workflows**. Then locate the **Configure REP ring (Non-Fabric)** card and click **Start**.

Alternatively, you can:

a. Navigate to the **Inventory** site topology view.

b. Click the device node on which you want to create the REP ring to view its details.

c. Click **REP Rings**, then click **Create REP Ring**.

Step 2 If a task overview window appears, click **Let's Do It** to start the workflow.

Step 3 In the **Select a root device** window, select the root device and then click **Next**.

Note The device must be reachable and have an upstream connection.

Step 4 In the **Select adjacent devices connected to root device** window, choose two adjacent devices that belong to the same ring and are directly connected to the root device:

a) Choose the first device, then click **Next**.

b) Choose the second device, then click **Next**.

Step 5 (Optional) Complete these tasks in the **Configure REP MACsec** window:

a) Check the **Enable MACsec** checkbox.

b) Configure the MACsec encryption key, then click **Next**.

Cisco MACsec encryption supports 128-bit and 256-bit AES encryption algorithms. These algorithms include the AES-GCM-128 and AES-GCM-256 cipher suites. The 128-bit AES encryption uses a 32-character hexadecimal key string, while the 256-bit AES encryption uses a 64-character hexadecimal key string.

Note To use the MACsec 256-bit cipher suite on Cisco Catalyst switches, a Network Advantage (NA) license is required.

Step 6 Complete these tasks in the **Review your REP Ring discovery selections** window:

a) Enter a name for the REP ring you are configuring.
b) Confirm that the root and adjacent devices you selected are displayed.
c) Confirm the MACsec configuration.
d) If necessary, click the appropriate **Edit** link to make changes.

Step 7 To initiate REP ring configuration, click **Provision**.

You can see a detailed status of the configuration progress on the **REP Ring Configuration Status** window.

Step 8 The **REP Ring Summary** window displays the details of the REP ring that is created along with the discovered devices. After the creation of the REP ring, a success message displays.

Step 9 To verify the creation of the REP ring, go to the **Inventory** window topology view and click any device that is part of the ring. In the slide-in pane, under the **REP Rings** tab, you can see the list of all REP rings that exist on that device.

Click a REP ring name in the list to view the REP ring details, such as the devices present in the ring, ports of each device that connect to the ring, and so on.

Add a node to a REP ring for nonfabric deployment

Use this procedure to add a single node to an existing REP ring. Nodes must be added one at a time.

Note You can use this feature on: Cisco IE 2000 Series Switches, Cisco Catalyst IE 3200 Rugged Series Switches, Cisco Catalyst IE 3300 Rugged Series Switches, Cisco Catalyst IE 3400 Rugged Series Switches, Cisco Catalyst IE 3400 Heavy Duty Series Switches, Cisco IE 4000 Series Switches, Cisco IE 4010 Series Switches, Cisco IE 5000 Series Switches, Cisco IE 9300 Series Switches, and Cisco Catalyst ESS3300 Embedded Series Switches.

Before you begin

Make sure you add the device to Catalyst Center. For information on how to add a device, refer to Add or edit a device, on page 596.

Procedure

Step 1 Onboard and claim the device using the Plug and Play workflow.

a) From the main menu, choose **Provision**> **Plug and Play**.

The **Plug and Play** window displays the onboarded device.

b) From the **Actions** drop-down list, click **Claim**.

c) In **Assign Site** window, click **Assign** to assign the device to the site in which you want to add the node and click **Next**.

d) Deploy the configuration to the device by clicking **Assign**, then click **Next**.

Note Plug and Play provisioning automatically deploys the device onboarding template. For more information, refer to Plug and Play provisioning overview, on page 585.

e) In the **Provision Templates** window, click **Preview Configuration** to review the configuration and click **Claim**.

f) Click **Ok** and **Yes**.

View the success message when you claim the device.

g) Click **Refresh**. Wait for the device onboarding process to complete. This process might take several minutes.

By default, the devices table refreshes every 30 seconds. Click the **Auto-Refresh** drop-down list and choose a refresh time.

The device moves to the **Provisioned** tab when the process completes.

Step 2 From the main menu, choose **Provision** > **Inventory**.

Step 3 Click **Refresh** and wait until the device is in managed state.

Step 4 Add the device to the REP ring.

a) Use the toggle button ( ) to switch to the Topology map view.

b) Click the REP and in the slide-in pane, click the **REP Rings** tab.

c) Under the **Actions** column, click the ellipsis and choose **Rediscover**.
The node insertion status is **Success** for successful addition of the device to the REP.

d) (Optional) In the **REP Rings** tab, click the **REP** link to view the steps executed. If a failure occurs, refer to the list to find the exact step where device insertion failed.

If the node insertion fails, rediscover the node.

Delete a node from a REP ring for nonfabric deployment

You can remove a node from an existing REP ring for nonfabric deployment.

These devices can be deleted from a REP ring:

- Cisco Industrial Ethernet (IE) 2000, 3100, 4000, 4010, and 5000 Series Switches
- Cisco Catalyst IE 3200, 3300, 3400, 3400H, 9300, 9310, and 9320 Rugged Series Switches
- Cisco Embedded Services 3300 (ESS3300), and 9300 (ESS9300) Series Switches
- Stratix 5400, 5410, and 5800 switches

The feature has limitations, including:

- If you remove an unreachable device and connect the other port of reachable devices instead of the REP-configured ports, REP discovery fails.
- You cannot delete the root device.
- If a REP ring contains both physical channels and port channels, deleting a node might break the REP ring.

Before you begin

Ensure that the REP ring to which the node belongs is complete.

Procedure

Step 1 Manually remove the device from the network.

Step 2 From the main menu, choose **Provision** > **Inventory**.

Step 3 Use the toggle button () to switch to the Topology map view.

If a REP ring has any unreachable devices (manually removed devices or devices that went down), you see a warning message.

Step 4 In the warning alert, click the REP ring link.
The slide-in pane for the corresponding REP ring opens.

Step 5 In the **REP Rings** tab, under the **Actions** column, hover your cursor over the ellipsis icon (•••) and click **Rediscover**.

Step 6 In the dialog box, click **Yes**.
The system removes the device from the REP ring, and updates the REP ring details.

MRP ring for nonfabric deployment

To ensure uninterrupted network connection, Media Redundancy Protocol (MRP) provides fault tolerance in industrial networks by continuously monitoring the status of your network links in a ring network topology.

MRP Media Redundancy Manager (MRM) defines its maximum recovery time for a ring in this range: 10 ms, 30 ms, 200 ms, and 500 ms.

MRP supports these Cisco Industrial Ethernet (IE) series switches: 3000, 4000, and 5000.

Note Currently, MRP ring support is not available for Cisco Embedded Services 9300 Switches (ESS9300).

Note

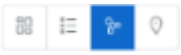
- The system supports multiple rings within an MRP ring. A single MRM can comprise up to three rings.
- By default, a maximum of 50 devices can be onboarded in a single MRP ring.
- MRP supports both trunk and access port configurations.

View MRP ring topology overlay

Use this procedure to view the Media Redundancy Protocol (MRP) ring status.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Select the toggle button () to switch to the Topology map.

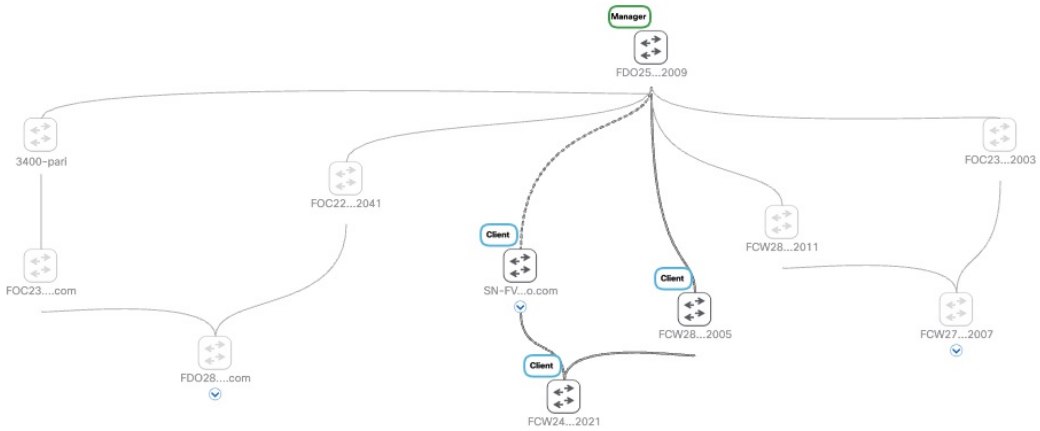
You can also view the MRP topology from the **Tools** > **Topology** window. In the hierarchy tree, select an area, site, building, or floor. Click the **Toggle Topology View** button in the top-right corner of the window.

Step 3 Filter the topology for MRM.

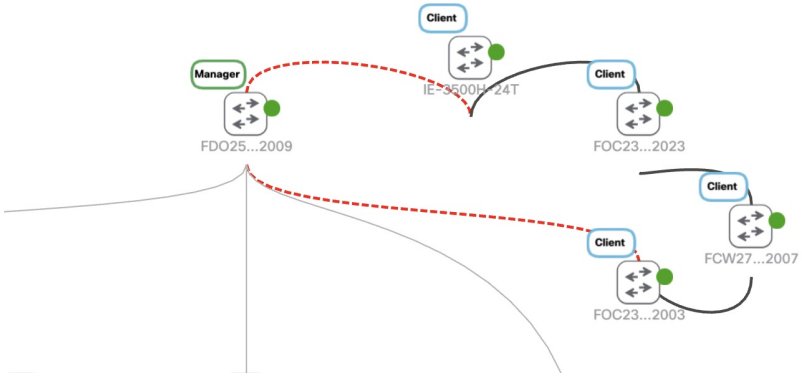
a) Click the **Filter** icon ( ).
b) Click the **Redundancy** > **MRP** radio button.
c) From the drop-down list, select the supported MRP manager device.
d) Click **Apply**.

Catalyst Center displays the MRP ring topology overlay that indicates the manager node, client nodes, and blocked ports.

The ports that are blocked are shown as black dashed lines.



The ports that are down, disabled, or not connected are shown as red dashed lines.



View MRP ring status for nonfabric deployment

Use this procedure to view the Media Redundancy Protocol (MRP) ring status.

Procedure

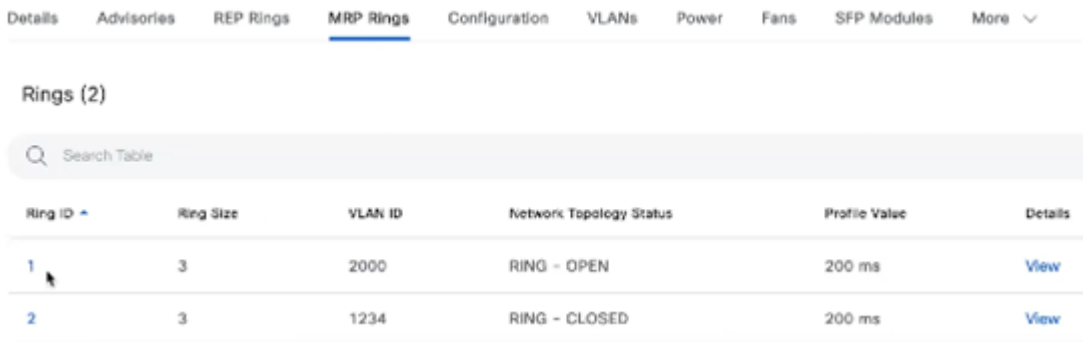
Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Use the toggle button ( ) to switch to the Topology map.

Step 3 To view MRP ring details, click anywhere on the ring, and then click the **MRP Rings** tab.

You can view the details listed in this table:

Field	Description
Ring ID	The number assigned by default
Ring Size	The number of devices in the ring
VLAN ID	The number assigned by default
Network Topology Status	This field displays one of these statuses: • Ring Open indicates a network connection failure. • Ring Closed indicates normal operation of the network.
Profile Value	Defines the maximum recovery time for the ring.



Step 4 Click the **Ring ID** to view these details:

Field	Description
Hostname	The hostname of the devices
Configuration Mode	The configuration mode of the devices
Operational Mode	This field displays one of these modes of operation: • Manager indicates that the device serves as MRM of the ring. The MRM initiates and controls the ring topology to react to network faults. It sends control frames on one ring port over the ring and receives them from the ring over its other ring port. The process also occurs in the opposite direction. • Client indicates that the device acts as a Media Redundancy Client (MRC). The MRC reacts to received reconfiguration frames from the MRM and can detect and signal link changes on its ring ports.
Port-1/Port-2	The interface name

Field	Description
Port-1/Port-2 Status	This field displays one of these statuses: • Disabled means ring ports drop all received frames. • Blocked means ring ports drop all received frames except MRP control frames and some standard frames such as LLDP. • Forwarding means ring ports forward all received frames. • Not Connected means the link is physically down or disconnected. (This state differs from Disabled state, where the MRP Port is manually disabled through software.)

Step 5 View the **Overview** of the MRP ring by clicking **View** hyperlink under **Details** column of the **Rings** table.

You can view details such as domain ID, domain name, priority, PROFINET or CLI managed, and port MAC address.

Parallel redundancy protocol

Parallel Redundancy Protocol (PRP) provides hitless redundancy (zero recovery time after a failure) in Ethernet networks.

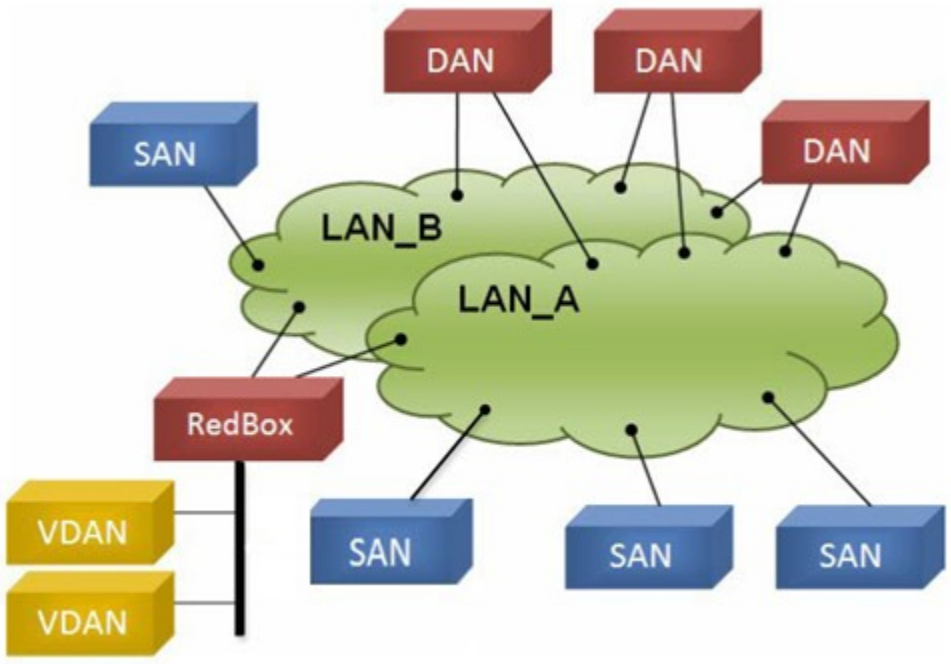
You can recover from network failures by configuring network elements in mesh or ring topologies using protocols like REP and MRP. With these redundancy schemes, the network typically recovers and resumes traffic flow within several milliseconds to several seconds.

Components of a PRP topology

PRP provides redundancy by connecting end nodes to two independent, disjointed, parallel networks (LAN-A and LAN-B). Each of these Dually Attached Nodes (DANs) has redundant paths to all other DANs in the network.

Singly Attached Nodes (SANs) are non-redundant endpoints in the network that attach only to either LAN-A or LAN-B.

A Redundancy Box (RedBox) is used in Parallel Redundancy Protocol (PRP) networks when an end node (device) does not have two network ports and does not implement PRP itself but still requires network redundancy. Such an end node can connect to a RedBox, which provides connectivity to the two different networks for the device. A node behind a RedBox appears to other nodes as a DAN and is referred to as a Virtual DAN (VDAN). The RedBox itself is a DAN and acts as a proxy on behalf of its VDANs.



View the PRP topology status

Use this procedure to view the Parallel Redundancy Protocol (PRP) status.

PRP topology characteristics:

- Applicable only to Cisco SD-Access deployments
- Ensure configurations are correct to display the proper LAN A and LAN B.

PRP works on Cisco Catalyst Industrial Ethernet 3400, 4000, 4010, and 9320 Series Switches.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

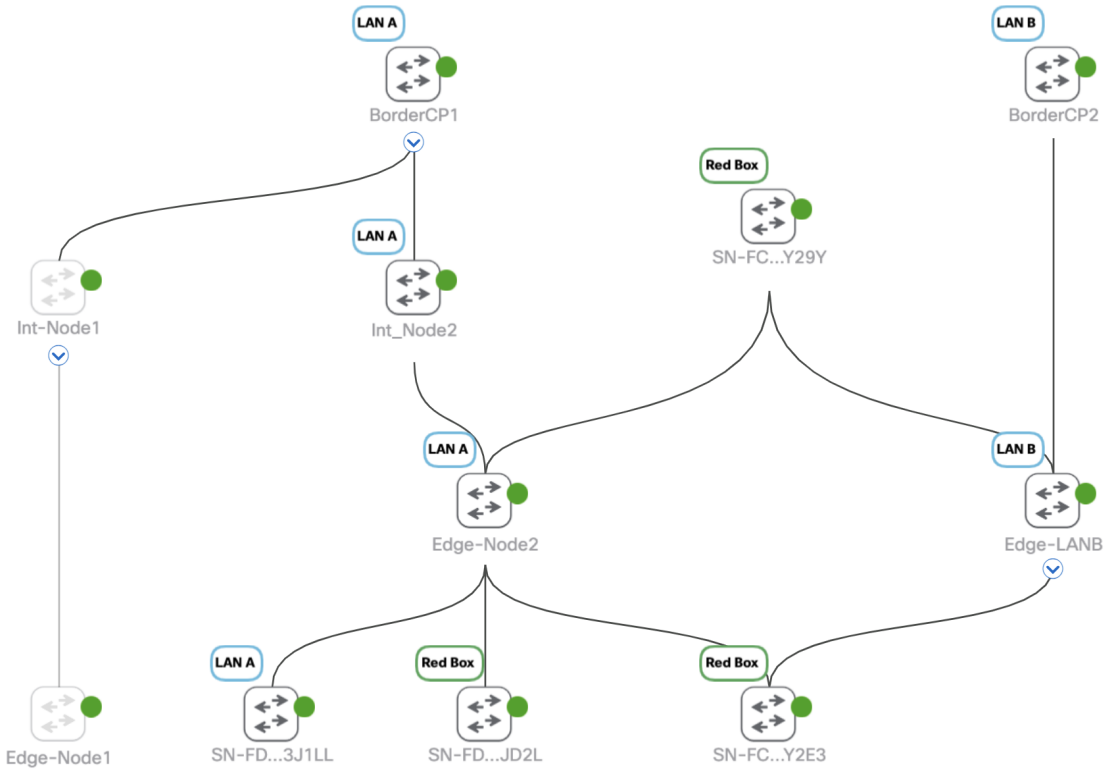
Step 2 Use the toggle button ( ) to switch to the topology view.

You can also view the PRP topology from the **Tools** > **Topology** window. In the hierarchy tree, select an area, site, building, or floor. Click the **Toggle Topology View** button in the top-right corner of the window.

Step 3 Filter the topology for devices labeled RedBox, LAN A, and LAN B.

a) Click the **Filter** icon ( ).
b) Click the **Redundancy** > **PRP** radio button.
c) From the drop-down list, choose **Show Redbox, LAN A, LAN B**.

The topology view displays the devices labeled RedBox, LAN A, and LAN B.



Note

- The nodes and links not participating in PRP are dim.
- The links that are down display as a red dotted line.

Create port groups

You can group ports based on an attribute or rule.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays device information gathered during the discovery process.

Step 2 To create a new port tag, click **Tag** and choose **Create New Tag**.

The **Create New Tag** slide-in pane is displayed.

Step 3 In the **Tag Name** field, enter the tag name. In the **Description** field, add a description for the tag.

Note The **WAN** tag is a reserved tag name. You can't create a new port tag named *WAN*, because the system autogenerates the WAN tag.

Step 4 In the **Tag Rules** area, click the **Port** tab.

Step 5 In the **Device Scope** area, click the drop-down list and choose **Location** or **Tag Name** of the device to define the filters.

Step 6 To add rules for tagging the ports, click the icon. You can tag the ports based on port status, speed, tag name, operational status, and description. You can add additional conditions using Boolean operators (AND, OR).

To delete a condition, click the delete icon.

Step 7 As the conditions are set, you can find the link for ports matching the condition at the bottom-left corner of the pane.

Click the link to view the ports. In the **Matching Ports** slide-in pane, you can view the device to which the port belongs and the port name.

Step 8 Click **Save**.

Assign tags to ports

You can manually assign tags to ports. For example, you can manually assign the system-generated **WAN** tag to a port.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Inventory** window, click a device name and choose **View Device Details**.

Step 3 In the left pane, expand **Interfaces** and click **Ethernet Ports**.

Step 4 In the top-right corner of the window, switch to the table view.

Step 5 Choose the port or ports to tag and click **Tag**.

Step 6 Choose the appropriate tags.

Step 7 Click **Apply**.

Port use information

You can check the last input received and last output sent by the port.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Devices** table, click a device name, and then click **View Device Details**.

The device details display in the window.

Step 3 In the left pane, choose **Interfaces** > **Ethernet Ports**.

Note This tab is available for all devices except APs.

Step 4 Click the port to view its details.

In the window, you can view the timestamp of **Last Input** received by the port and **Last Output** transmitted by the port.

Maintenance mode for devices

Schedule maintenance for devices

You can place one or more devices under maintenance mode in Catalyst Center. If a device is placed under maintenance mode, Catalyst Center will not process any telemetry data associated with the device. Placing faulty devices under maintenance mode prevents unnecessary alerts.

Note When devices are in maintenance mode, you cannot collect information and do polling operations.

Note While scheduling the maintenance mode for Cisco Wireless Controllers and APs:

- When you schedule maintenance for a Cisco Wireless Controller, all the APs associated with the wireless controller are moved under maintenance mode with the same schedule.
- When a wireless controller is in maintenance mode, you cannot modify the maintenance schedule of a single AP associated with the wireless controller. The system displays a warning message indicating that the device is already scheduled for maintenance. If you modify the schedule of the wireless controller, then all the APs under the wireless controller will be impacted.
- When the wireless controller is not in maintenance mode, you can select the APs individually and schedule them for maintenance.
- When an AP moves from one wireless controller to another, the maintenance mode is impacted accordingly:
  - If the AP is moving from a wireless controller that is in maintenance mode to a wireless controller that is not under maintenance, then the AP will not have maintenance mode after moving.
  - If the AP is moving from a wireless controller that is not in maintenance mode to a wireless controller that is under maintenance, then the AP will be in maintenance mode after moving.
  - If the AP is in maintenance mode and is moving from a wireless controller that is not under maintenance mode to a wireless controller that is also not under maintenance, then the AP will retain its maintenance mode after moving.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Choose the devices for maintenance scheduling.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Schedule Maintenance**.

The **Schedule Maintenance** slide-in pane is displayed.

Step 4 In the **Reason For Maintenance** field, enter a reason for placing the device under maintenance mode.

By default, Catalyst Center adds a reason, and you can modify it.

Step 5 In the **Define Maintenance Window** area, do this step:

a) Choose the start date and time for maintenance.
b) Choose the end date and time for maintenance.
c) Alternately, click **Days/Hours** and enter days and hours for maintenance.

Note To choose recurrence for maintenance, choose the **Days/Hours** option.

Step 6 In the **Maintenance Recurrence** area, click **None**, **Daily**, or **Weekly**.

- **None**: Maintenance will not recur.
- **Daily**: Enter the interval in days in the **Run at Interval (Days)** field.
- **Weekly**: Enter the interval in weeks in the **Run at Interval (Weeks)** field.

Step 7 If you have chosen **Daily** or **Weekly** for recurrence, check the **Set Schedule End** check box.

Step 8 Click **End Date** or **End After (Occurrences)**.

- **End Date**: Enter month, date, and year for maintenance end.
- **End After (Occurrences)**: Enter the number of occurrences after you want maintenance to end.

Step 9 In the **Maintenance Time Zone** area, choose a time zone for maintenance.

Step 10 Click **Submit**.

Manage maintenance schedule for devices

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 From the **Actions** drop-down list, choose **Inventory** > **Manage Maintenance**.

The **Manage Maintenance** slide-in pane appears. The **Status** column shows the current status of maintenance schedules.

Step 3 Click the **Search** icon to search maintenance schedules or **Filter** icon to filter maintenance schedules.

Step 4 In the **Actions** column, click the **Edit** icon to edit the maintenance schedule.

Note For in-progress maintenance schedules, you can only extend the maintenance end time.

Step 5 Click the **Delete** icon in the **Actions** column to remove the maintenance schedule.

Note You cannot delete in-progress maintenance schedules.

Remove a device from maintenance

You can remove a device from maintenance after completing scheduled maintenance.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 From the **Actions** drop-down list, choose **Inventory** > **Exit Maintenance**.

Step 3 In the **Exit Maintenance** window, click **Confirm**.

Note Maintenance windows operate independently of individual device assignments. After a maintenance window is initiated, it will continue for its full duration, even if a device is removed from it. To schedule a new maintenance window for that device, you must either:

- Wait for the current maintenance window to finish.
- Edit the existing maintenance window to end at an earlier time.

Inventory Insights

The **Inventory Insights** window displays devices that have configuration inconsistencies with other directly-connected devices. It also displays devices that are misconfigured, as compared with the Catalyst Center best-practice recommendations. Additionally, you can view whether the link between the devices is up (active) or down (inactive), a link is down when the connection between devices no longer exists. Historical data is retained for future reference.

For example, assume that there is a network link between *device A* and *device B*. If you remove the link from *device B* and connect it to a new *device C*:

- The old link between *device A* and *device B* remains present and can be manually deleted by the user from the **Tools** > **Topology** window. No action is required by the user on the **Inventory Insights** window, it is shown to retain the historical data for your reference.
- The new link between *device A* and *device C* is shown as up.

Catalyst Center provides insights with suggested actions.

Speed and duplex settings mismatch

Catalyst Center displays devices that are connected but have different speed and duplex values configured at each end of a device link.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory Insights**.

The **Inventory Insights** window appears.

Step 2 Click **Speed/Duplex settings mismatch** to view the suggested actions that can be done on devices.

The suggested actions appear in the right pane.

Step 3 Click the number of instances to see the mismatches.

The **Speed/Duplex settings mismatch** window highlights the mismatches of speed and duplex.

Step 4 Make the required changes to the device configuration by doing the suggested actions.

VLAN mismatch

Catalyst Center shows devices that are connected to each other but are set to different VLANs on either end of a device link.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory Insights**.

The **Inventory Insights** window displays.

Step 2 Click **VLAN Mismatch** to see the suggested actions that can be done on devices.

The suggested actions appear in the right pane.

Step 3 Click the number of instances to see the mismatches.

Step 4 Update the device configuration according to the suggested actions.

Manage system beacon

You can highlight switches in the Catalyst Center inventory by using system beacons.

You can enable a system beacon on these devices:

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Ethernet Stackable Switches

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays device information gathered during the discovery process.

Step 2 Select the devices for which you want to enable or disable beacons.

Note
- You can enable beacons on up to five standalone devices at a time.
- To enable beacons on stacked devices, you must select only one device at a time. For a stacked device, you can enable beacons on one or more stack members.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Manage System Beacon**.

Step 4 In the **Manage System Beacon** slide-in pane, click the **Enabled** radio button under **System Beacon State** and then click **Apply** to enable a beacon on the chosen devices.

After the system beacon is enabled, a blue beacon icon ( ) appears next to the device name in the inventory.

Step 5 (Optional) If you have selected a stacked device, do these steps in the **Manage System Beacon** slide-in pane:

a) Check the **Update System Beacon Status?** check box corresponding to the stack members on which you want to enable the beacon.
b) Under **System Beacon State**, click the **Enabled** radio button.
c) Click **Apply**.

Step 6 (Optional) To disable a beacon on the selected devices, do these steps in the **Manage System Beacon** slide-in pane:

a) Under **System Beacon State**, click the **Disabled** radio button.
b) Click **Apply**.

Alternatively, in the **Inventory** window, place the cursor over the blue beacon icon ( ) next to the device name and click **Disable**.

Device roles

Catalyst Center assigns device roles

- to identify and group devices,
- to determine if specific configurations are pushed to the devices, and
- to determine the device placement on the network topology map.

Automatic roles are assigned statically or dynamically:

- Static assignment: Certain devices receive fixed roles based on their platform ID or device family; these roles do not change.
- Dynamic assignment: Other devices receive roles based on network changes and their relationships with neighboring devices.

Manual roles are assigned by users in the Catalyst Center GUI. Manual role assignment takes precedence over automatic role assignment. Automatic role assignment runs periodically as part of the topology change process.

This table shows each device role and its position in the network topology.

Table 39: Device roles and topology positions

Topology position	Device role
Tier 1	Internet (not configurable)
Tier 2	Border Router
Tier 3	Core
Tier 4	Distribution
Tier 5	Access
Tier 6	Unknown

Change the device role manually

Use this procedure to change the device role manually from the **Inventory** window.

For more information about device roles, refer to Device roles, on page 179.

Note

- When you manually change the device role, the assignment remains static. The device role is not updated during subsequent device resynchronizations, even if a change is detected. After a manual change, you must also manage the device role manually.
- When the **Access** role is manually or automatically assigned to a device, , either manually or automatically, IP Device Tracking (IPDT) is configured or removed based on the site's IPDT settings.

Before you begin

Make sure that you have devices in your inventory. If you do not have devices in your inventory, use the Discovery feature to add them.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Inventory** table, check the check box next to the device whose role you want to change.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** slide-in pane, update the device role.

a) Click the **Device Role** tab.

b) From the **Device Role** drop-down list, choose an appropriate role.

c) Click **Update**.

Update a device management IP address

You can update the management IP address of a device.

Note Update one device at a time. You cannot update the management IP address for Meraki devices.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Select the device that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

The **Edit Device** slide-in pane appears.

Step 4 Click the **Management IP** tab, and enter the new management IP address in the **Device IP/ DNS Name** field.

Note Make sure that the new management IP address is reachable from Catalyst Center. Also, verify that the device credentials are correct. If these conditions are not met, the device might become unmanaged.

What to do next

Reprovision the device to update the source-interface configuration.

Update the device polling interval

You can update the polling interval globally for all devices by choosing **System** > **Settings** > **Network Resync Interval**. To update the polling interval for a specific device, select **Device Inventory**. The value set using **Network Resync Interval** replaces any value configured in **Device Inventory**.

If you do not want a device to be polled, you can disable polling.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Select the devices to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** slide-in pane, click **Resync Interval**.

Step 5 Select the resync type.

Note
- To set the resync type as global, go to **System** > **Settings**.
- The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Catalyst Center continues to use the device-specific polling time.

Step 6 In the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles.

Step 7 Click **Update**.

Resynchronize device information

You can immediately resynchronize device information for selected devices, regardless of the interval configured for device resynchronization.

Note The number of devices that can be resynchronized at the same time depends on device configuration size and the number of associated APs. In environments with thousands of APs, resource contention might cause sync requests to queue and process based on priority.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Select the devices for which you want to gather information.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Resync Device**.

Note When the resync is done for a specific device, the debug log is enabled automatically for that device, and XDE and device pack logs are collected under **System** > **System 360** > **Cluster Tools** > **Monitoring** or **Log Explorer**.

Step 4 Click **OK**.

Delete a network device

Use this procedure to delete a network device from Catalyst Center.

You can delete devices that aren't a part of the fabric network from the Catalyst Center database.

Note
- If the device is a part of the fabric network, you can't delete it. Remove the device from the fabric network, and then delete it from the inventory. For detailed steps, see Remove a device from a fabric, on page 1025.
- When you remove a wireless sensor from the inventory, the sensor resets to factory defaults. When the sensor rejoins, it gets the current configuration.

Before you begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box next to the device or devices that you want to delete.

Note You can select multiple devices by checking additional check boxes, or select all the devices by checking the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Delete Device**.

Note When you delete devices integrated with Cisco ISE, the deleted devices are moved to new Network Device Group (NDG) group in Cisco ISE.

Step 4 (Optional) In the **Warning** window, check the **Config Clean-Up** check box.

The Device Controllability workflow is triggered. The network settings and telemetry configuration are removed from the selected device. For more information, see "Device Controllability" in the Cisco Catalyst Center Administrator Guide.

Note When you check this check box for a wireless controller that is provisioned through Catalyst Center, all AAA-related commands are deleted, including the commands that were manually configured on the wireless controller before it was discovered in Catalyst Center.

- To keep the AAA configurations during device deletion, do not check this check box.
- To view which AAA commands are deleted, manage AAA configurations in Catalyst Center.

Step 5 Click **OK** to confirm the action.

Launch Command Runner (Inventory)

You can launch the Command Runner application for selected devices in the **Inventory** window.

Before you begin

Install the Command Runner application. For more information, refer to the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Select the devices on which you want to run commands.

Step 3 From the **Actions** drop-down list, choose **More** > **Command Runner**.

For information about the commands that you can run and how to run them, refer to Run diagnostic commands on devices, on page 581.

Troubleshoot device reachability issues using Run Commands

You can launch the **Run Commands** window from the **Inventory** window and run platform commands, such as ping, traceroute, and snmpget, to troubleshoot device reachability issues.

Note If you want to execute the platform commands directly on a Catalyst Center cluster, do not select any device before launching **Run Commands**. Selecting a device causes the commands to execute for that device instead of the platform.

Before you begin

Install the Command Runner application. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 From the **Actions** drop-down list, choose **More** > **Run Commands**.

You can enter **`man`** anytime to retrieve a list of currently supported commands and shortcuts.

Use a CSV file to import and export device configurations

CSV File Import

You can use a CSV file to import your device configurations or sites from another source into Catalyst Center. To download a sample template, complete these steps:

1. Go to the **Inventory** window and click **Add Device**.
2. In the **Add Device** slide-in pane, click **Import Inventory**.
3. Click **Download Template** to download a sample CSV file template.

When you use a CSV file to import device or site configurations, the extent to which Catalyst Center can manage your devices depends on the information you provide in the CSV file. If you do not provide values for CLI username, password, and enable password, Catalyst Center will have limited functionality and cannot modify device configurations, update device software images, or do other important functions.

You can specify the credential profile in the CSV file to apply the corresponding credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, the manually entered credentials take higher priority. Management uses a combination of the manually entered credentials and the credential profile. For example, if the CSV file contains a credential profile with SNMP and SSH or Telnet credentials in addition to manually entered SNMP credentials, the device is managed based on the manually entered SNMP credentials and the SSH or Telnet credentials in the credential profile. For security, use SSH rather than Telnet.

Note You also must provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 username and authorization password.

For partial inventory collection in Catalyst Center, you must provide these values in the CSV file:

- Device IP address
- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value

For full inventory collection in Catalyst Center, you must provide these values in the CSV file:

- Device IP address
- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value
- Protocol
- CLI username
- CLI password
- CLI enable password
- CLI timeout value

CSV File Export

Catalyst Center enables you to create a CSV file that contains all or selected devices in the inventory. When you create this file, you must enter a password to protect the configuration data that the file will contain.

Import device configurations from a CSV file

You can import device configurations from a CSV file.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Click **Add Device**.

Step 3 In the **Add Device** slide-in pane, click **Import Inventory** to import device credentials.

Step 4 In the **Import Inventory** slide-in pane, drag and drop the CSV file into the boxed area. Alternatively, click **Choose a file** and browse to the CSV file.

Step 5 Click **Import**.

Export device data

You can export specific data pertaining to selected devices to a CSV file. The CSV file is compressed. Click **Export** to export the data of filtered devices or all devices.



Caution Handle the CSV file with care because it contains sensitive information about the exported devices. Ensure that only users with special privileges perform a device export.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 To export configuration information for only certain devices, check the check box next to the devices that you want to include. To include all devices, check the check box at the top of the device list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Export Inventory** to export the device configurations.

The **Export Inventory** dialog box appears.

Step 4 In the **Password** field, enter a password that will be used to encrypt the exported CSV file.



Note The password is required to open the exported file.

Step 5 Confirm the encryption password.

Step 6 Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.

Step 7 Click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Export device credentials

You can export device credentials to a CSV file. You are required to configure a password to protect the file from unwanted access. You need to supply the password to the recipient so that the file can be opened.

Caution Handle the CSV file with care because it lists all of the credentials for the exported devices. Ensure that only users with special privileges do a device export.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Check the check box next to the devices that you want to include in the CSV file. To include all the devices, select the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Export Inventory**.

The **Export** dialog box appears.

Step 4 In **Select Export Type**, click the **Credentials** radio button.

Step 5 Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.

Step 6 In the **Password** field, enter a password that will be used to encrypt the exported CSV file.

Note The password is required to open the exported file.

Step 7 Confirm the encryption password and click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Configuration drift of a device

Configuration changes made on devices are saved in the internal Catalyst Center server. For information on how to view the configuration drift, see View configuration drift of a device, on page 190.

Configuration drifts are captured when these events occur:

- First Time Collection: On adding a device to Catalyst Center, device configuration is collected.
- Syslog-Based Collection: Catalyst Center monitors Syslog events sent by devices, and identifies the configuration changes. The configuration archive is triggered after 2 minutes, on occurrence of the latest event. Based on the login IP Address in Syslog events, configuration drifts are marked in-band (configuration changes done by Catalyst Center) or out-of-band (configuration changes done outside Catalyst Center).



Note

- Catalyst Center must be configured as a Syslog server, from **Design** > **Network Settings** > **Telemetry** > **Syslogs** for Syslog-Based collection to work. For more information, see Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 43.
- New traps within the 2 minutes window will restart the timer to avoid multiple archives with partial changes. For accurate results, we recommend you to wait for at least 2 minutes.

- Daily Backup Collection: Catalyst Center performs automated backup of device configurations that is scheduled to run every day at 11:00 p.m. (UTC time zone). During this process, Catalyst Center compares the timestamp of the last device configuration collection with the timestamp of the device configuration archived. If the difference is more than 30 minutes, the device configuration archive runs.
- Weekly Backup Collection: Catalyst Center performs periodic weekly backup of device configurations, that is scheduled to run every Sunday at 11:30 p.m. (UTC time zone). When none of the above mentioned events are received for a device, the configuration changes that are done outside Catalyst Center or in Catalyst Center are captured by the weekly backup archive. For more information, see "Configure Device Configuration Backup Settings" section in Cisco Catalyst Center Administrator Guide.



Note Configuration drifts detected by weekly backup archive are classified as in-band (configuration changes done by Catalyst Center), even though it is possible that the configuration changes were done outside Catalyst Center.

Note

- If number of config drifts saved for the device exceeds the value set in **System** > **Settings** > **Device Settings** > **Configuration Archive** > **Internal** window, the oldest configuration is automatically deleted to create space for the new configuration to be archived. The default value of configuration drift that can be saved per device is 15 and the maximum value is 50.
- Disk use is optimized by ignoring the collected archive when no changes are present. Disk space optimization is not applicable for the First Time Collection.

View configuration drift of a device

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Devices** table, click the device name. More information about the device is displayed.

Step 3 Click **View Device Details** hyperlink.

The device details are displayed in the window.

Step 4 In the left pane, click **Config Drift**.

The **Configuration Changes** window appears and you can view this information:

- **Total config drifts being saved**: Shows the number of configuration drifts saved per device that includes labelled configs.

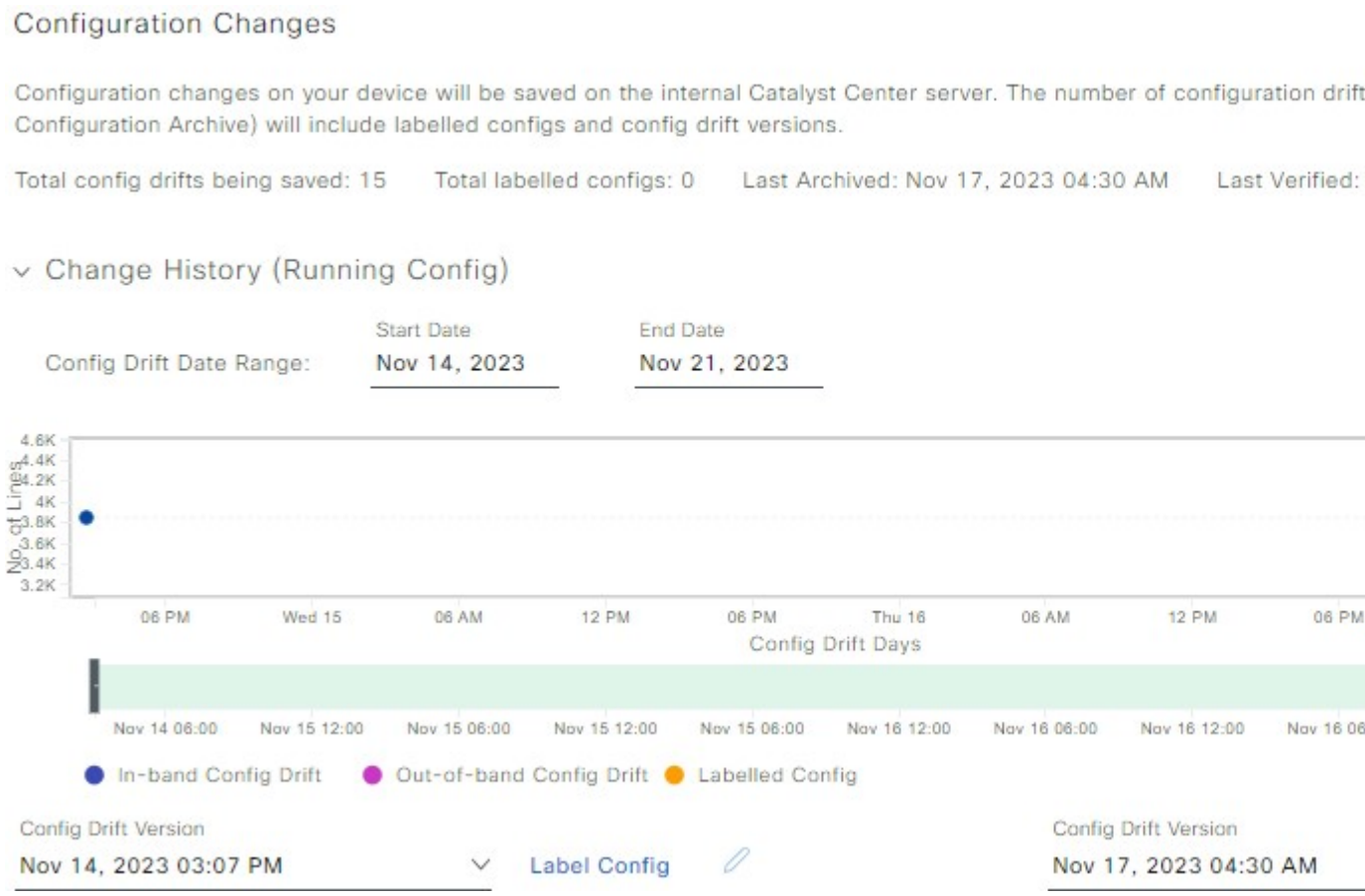
  You can change the number of config drifts being saved per device from **System** > **Settings** > **Device Settings** > **Configuration Archive** window.

- **Total labelled configs**: Shows the number of labelled configs for the device.
- **Last Archived**: Shows the timestamp of the last configuration archived. This timestamp ensures that the users have access to the most up-to-date configuration data. Also, by knowing the specific time of the last configuration archived, you can track changes and identify potential issues or discrepancies.

  For information on how to archive the configuration of your network devices, see "Configure Device Configuration Backup Settings" section in Cisco Catalyst Center Administrator Guide.

- **Last Verified**: Shows the timestamp of the config-drift verification that was performed when an event was received by the system. The event refers to first time collection, syslog-based collection, daily backup collection or weekly backup collection that is described in the previous section.

  The last verified timestamp allows you to monitor when the check was last performed, ensuring the devices are continuously monitored for configuration inconsistencies.



Step 5 Expand the **Change History** tab to view these details:

a) **Config drift date range**: Click the **Start Date** and **End date** to choose the date range for which you want to view the config drift. By default, the start and end dates are set to display the config drift for the last 15 days.

b) **Config drift timeline graph**: Shows the config drift for the chosen date range. By default, the last 15 days of config drift are shown in the timeline graph.

The timeline graph shows these details:

- **In-band Config Drift**: Configuration changes done by Catalyst Center are shown as a blue bubble in the timeline graph.
- **Out-of-band Config Drift**: Configuration changes done outside Catalyst Center are shown as a purple bubble in the timeline graph.
- **Labeled Config**: The config version labeled and archived in Catalyst Center is shown as an orange bubble in the timeline graph. For more information, see Label configuration drift, on page 192.

c) **Config Drift Version**: Click the down arrow to view all the available config drift versions.

d) **Running Config**: Click the config drifts on the timeline graph. The comparison is shown under the **Running Config** tab. The differences between the config versions are marked in different colors for better visibility.

Label configuration drift

You can label the config drift on the timeline graph for future reference. The labeled config drift will never be deleted unless it is unlabeled.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name, and more information about the device displays.

Step 3 Click **View Device Details**.

Device details display in the window.

Step 4 In the left pane, click **Config Drift**.

The **Configuration Changes** window displays.

Step 5 Choose the config drift in timeline graph that you want to label. The timestamp of the chosen config drift shows in the **Config Drift Version** below the timeline graph.

Step 6 Click **Label Config** corresponding to the chosen config drift version.

Step 7 In the **Label Configuration** window, enter a name for the config version. The prefix of the label config is fixed as CCA_.

Note Do not use special characters for the config version name.

Step 8 Click **Save**. The labeled config drift is shown in orange in the timeline graph.

Note

- If the number of labeled config versions is greater than the chosen range, change the total number of config drifts to be saved. For more information on how to configure the number of config drifts to be saved, see the "Configure Device Configuration Backup Settings" section in the *Cisco Catalyst Center Administrator Guide*.
- Catalyst Center permits the labeling of up to 80% of the total configuration drift. When a user reaches this 80% threshold in labeled configurations drift, a warning banner displays at the top of the **Configuration Changes** window.

Step 9 To remove the label, select the labeled config version and click **Remove label**.

Visibility and control of device configurations

The **Visibility and Control of Configurations** feature provides a solution to further secure your planned network configurations before deploying them onto your devices. With enhanced visibility, you can enforce the previewing of device configurations (CLI and NETCONF commands) before deploying them. With enhanced control, you can ensure only authorized configurations are provisioned onto your network devices through an IT Service Management (ITSM) check. These two options also offer you the flexibility to preview configurations at your own pace. You can preview the configurations immediately in a visibility- and control-supported workflow or later in the **Activities** > **Tasks** window.

By default, the **Visibility and Control of Configurations** settings include this configuration:

- Visibility of Configurations (**Configuration Preview**) is enabled.
- Control of Configurations (**ITSM Approval**) is disabled.

To enable or disable these settings, see "Enable Visibility and Control of Configurations" in the *Cisco Catalyst Center Administrator Guide*.



Note If a provisioning workflow supports **Visibility and Control of Configurations**, this banner message displays when you schedule the deployment of your task:

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to **System** > **Settings** > **Visibility and Control of Configurations**.

Visibility and Control of Configurations workflow

When you schedule your task during a provisioning workflow, the Visibility and Control of Configurations settings determine your scheduling and preview options.

When **Configuration Preview** is enabled:

- The **Preview** check box is checked and enforced.
- Schedule the task **Now** or **Later**.
- Name the task.
- You must preview the device configurations before deploying them.

When **Configuration Preview** and **ITSM Approval** are enabled:

- The **Preview** check box is checked and enforced.
- Schedule the task **Later**.
- Name the task and add details for the IT administrator in the **Notes** field.
- You must preview the device configurations and submit them for approval before the deployment.

When **Configuration Preview** and **ITSM Approval** are disabled:

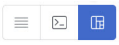
- The **Preview** check box is checked and optional.
- Schedule the task **Now** or **Later**.
- Name the task.
- You can deploy the device configurations without previewing them or submitting them for approval.

If you check the **Preview** check box, Catalyst Center does these steps:

	Step	Description
1	Catalyst Center performs a set of network provisioning prechecks to ensure a seamless provisioning operation.	On the **Performing Initial Checks** window, Catalyst Center checks for and notifies you of any Pending Operations and Device Compliance issues. You must address all the identified issues and do a recheck to ensure all the validations are successful. For more information, see Network provisioning prechecks, on page 202.
2	Catalyst Center prepares the chosen devices to generate the configurations.	On the **Preparing Devices and Configuration Models** window, if the provisioning workflow supports the workflow progression view, the steps the system takes to prepare a listed device display. Otherwise, an in-progress message displays. Because this preparation step can take some time, you can exit the workflow and return to it later while the system continues the process in the background.
3	Catalyst Center displays the device configurations for the first listed device.	On the **Preview Configuration** window, Catalyst Center displays a side-by-side comparison of the running configuration and the planned configuration for the first listed device. You can review the device configurations and then, when you're ready, deploy them or submit them for ITSM approval.

While reviewing the configurations on the **Preview Configuration** window, you can do these tasks:

To...	Do this...
Preview a device's configurations.	Choose a device in the left pane.
Filter the data in the configuration preview pane.	From the **View by Configuration Source** drop-down list, choose an available option.
View a side-by-side comparison of the planned configuration and the running configuration, or view only the planned configuration.	Click the view switcher (). **Note** Viewing YANG configurations in the side-by-side comparison view isn't supported.

To...	Do this...
Highlight corresponding commands between the running and planned configurations.	Click one command in one configuration to highlight the corresponding command in the other configuration. **Note** Keep these limitations in mind: • The system supports only side-by-side highlighting for first-level commands, not sublevel commands. • All commands must be a complete match for the system to display the side-by-side highlighting between configurations. • If you click any commands starting with `No` in one configuration, the system will ignore the `No` portion when checking for a match in the other configuration.
Search for a value in the displayed configuration.	Use the **Search configuration** field.
Preview the YANG configuration in a tree view for Cisco Catalyst 9800 Series Wireless Controllers.	Click the **Tree View** () button. **Note** The **View by Configuration Source** drop-down list isn't available in the tree view.

To...	Do this...
Generate the IOS CLI from the YANG configuration for Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.15.1 or later.	

To...	Do this...

	Click the **Generate CLI from Yang Configuration** () button.
	Note
	Keep these limitations in mind:
	• The time taken to generate the IOS CLI varies based on the scale of your network and the type of the current operation.
	• IOS CLI generation from YANG configuration isn't supported for Embedded Wireless Controller on Catalyst 9000 Series Switches
	• If the Candidate Configuration feature with candidate datastore is enabled on the wireless controller, IOS CLI generation from the YANG configuration isn't supported.
	• When you modify a configuration and generate the IOS CLI, the CLI change on the device after applying the YANG configuration displays in the configuration preview. You can't use the generated CLI on the wireless controller.
	For example, if the current device configuration already matches the YANG configuration, the generated IOS CLI in the configuration preview doesn't contain any commands.
	• If the validation fails, the IOS CLI isn’t generated from the YANG configuration in the configuration preview.
	• The admin state for some of the objects must be changed to the **shutdown** state before applying the modified configuration. The admin state of the object is returned to the **no shutdown** state at the end of the CLI sequence for such modifications. For these configurations, the configuration preview doesn't contain the CLIs in sequence for the **shutdown** command.
	For example, for configuring the media stream, broadcast SSID, and radio in WLAN, the YANG configuration handles the shutdown and activation internally. This is an example of the ideal CLI sequence for this configuration:
	`wlan test4`
	`shutdown`
	`broadcast-ssid`
	`dot11bg 11g`
	`media-stream multicast-direct`
	`no shutdown`

To...	Do this...

	However, the CLI generated from the YANG configuration may not include the **shutdown** command. This is an example CLI generated from the YANG configuration:
	`wlan test4`
	`broadcast-ssid`
	`dot11bg 11g`
	`media-stream multicast-direct`
	`no shutdown`
	Therefore, the CLI generated in the configuration preview may not work on the wireless controller when used in Virtual TeleType (VTY).

Display the workflow progression view.	Choose a device in the left pane, and then click **Back to workflow progress** in the top-right corner of the right pane. To return to the configuration preview pane, click **Go to generated config**. **Note** **Back to workflow progress** and **Go to generated config** are only available if the workflow supports the workflow progression view.
Exit the workflow and review the device configurations later.	Click **Exit and Preview Later**. When you're ready to continue reviewing the configurations, go to the **Activities** > **Tasks** window and open the relevant work item.

After reviewing the configurations, depending on the **Visibility and Control of Configuration** settings, you can do these tasks:

To...	Do this...
Discard the work item permanently.	Click **Discard** and, in the **Discard** dialog box, click **Accept**. **Note** • After discarding it, it is permanently discarded after two weeks. • After discarding the configuration preview, you can still view the completed configuration preview for the relevant devices. This visibility allows you or your IT administrator to inspect any issues related to the device configurations.

To...	Do this...
Deploy the configurations or submit them for ITSM approval.	Click **Deploy** or **Submit for ITSM Approval**. **Note** • If **Save Intent** displays instead of **Deploy**, the parameters that you chose during the workflow are already present on the device. To save those parameters to the database, click **Save Intent**. No configuration is pushed to the device because the device already has the required configuration. • If there are multiple devices, you must click each device to preview its configuration. However, when you click **Deploy**, the configurations are pushed to all the devices even if the configurations have not been previewed on all devices. In the slide-in pane, schedule the time and date of the deployment and, if you're submitting the configurations for ITSM approval, add notes for the IT administrator. Then click **Submit**. **Note** For a provisioning task, after deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name). You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it is deployed at the scheduled time. **Note** When you preview the configurations, Catalyst Center creates a snapshot of the configuration previews. If there are any changes in the network settings or network profiles after this operation is scheduled for deployment, the changes are not included during the device provisioning.

Deploy your device configurations now or later

At the scheduling step of a workflow that supports Visibility and Control of Configurations, complete this procedure to deploy your device configurations immediately or at a later time.

Procedure

Step 1 From the scheduling page, do these steps:

a. Ensure that the **Preview** check box is unchecked.

Note If **Preview** is checked, the deployment follows the preview-first flow. For instructions, refer to Preview and deploy your device configurations, on page 200.

b. Under **Deploy**, click **Now** or **Later**.

c. Update the task name if needed.

d. Click **Apply**.

Step 2 On the **Performing Initial Checks** window, prepare and submit the task for deployment.

a) Address all the issues to deploy the device configurations.

Ensure all validations are successful by clicking **Recheck**.

b) Click **Submit**.

The device configurations deploy at the scheduled time. View the task in the **Tasks** window.

Preview and deploy your device configurations

When you reach the scheduling step in a workflow that supports Visibility and Control of Configurations, complete this procedure to preview and deploy your device configurations.

Before you begin

Ensure that Visibility and Control of Configurations is enabled in the settings. For more information, see Visibility and control of device configurations, on page 193.

Procedure

Step 1 From the scheduling page, do these steps:

a. Check the **Preview** check box.

b. Under **Deploy**, click **Now** or **Later**.

c. Update the task name if needed.

If **ITSM Approval** is enabled, provide notes for the IT administrator.

d. Click the confirmation button (for example, **Apply**).

Note The button label may vary by workflow.

Step 2 On the **Performing Initial Checks** window, address all the issues and then click **Next** to continue with your current deployment.

Ensure all validations are successful by clicking **Recheck** in the lower right corner of the window.

Step 3 On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations.

Tip This preparation can take some time. You can click **Exit and Preview Later** and view the work item in the **Tasks** window.

Step 4 In the **Preview Configuration** window, complete these steps:

a) Review the device configurations.

b) Choose a deployment option.

Click...	To...
Deploy or **Submit for Approval**	deploy the device configurations.
Exit and Preview Later	review and deploy the device configurations later. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

c) If the scheduled deployment time has passed, reschedule the deployment.

In the **Confirm deployment time** dialog box, reschedule it to run **Now** or **Later** if **ITSM Approval** is disabled, or **Later** if **ITSM Approval** is enabled. Then click **Confirm**.

You can check the work item approval status or the task deployment status on the **Tasks** window. If it is not approved, resubmit the work item for ITSM approval. When it is approved, the item is deployed at the scheduled time.

Note After submitting the task, view the progress of the provisioning task with the **Task Progress** bar in the **Activities** > **Tasks** window by clicking the task name.

Network provisioning prechecks

To ensure a seamless provisioning operation, Catalyst Center runs a set of prechecks to ensure that there are no pending operations that might conflict with the current task and devices are compliant.

Note This feature is only applicable for provisioning, SWIM, and RMA workflows.

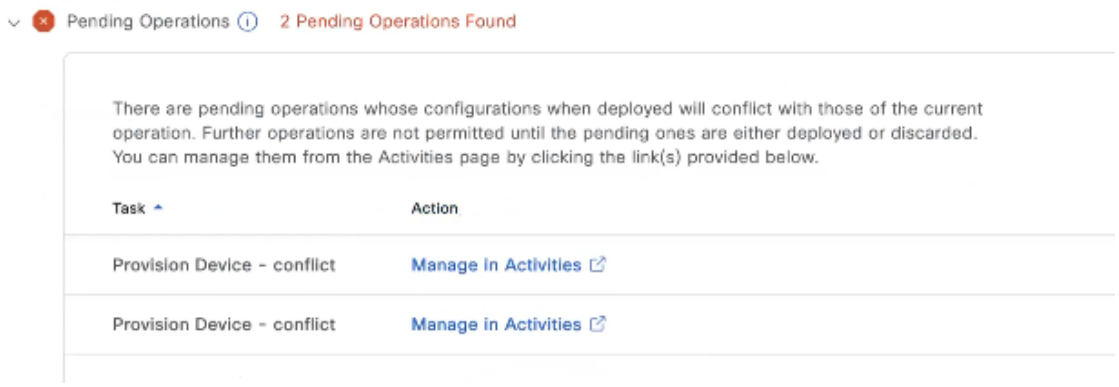
The prechecks are run during any provisioning workflow after you schedule the configuration deployment by choosing the **Now** or **Later** option or after choosing the **Preview and Deploy (Recommended)** option, if applicable.

On the **Performing Initial Checks** window, Catalyst Center notifies you of any issues, including:

Item	Description
icon	This icon indicates that there are no errors, and you can click **Next** or **Submit** to proceed with provisioning.
icon	This icon indicates that you must address all the issues to proceed with provisioning.
icon	This icon indicates that the issue needs your attention. You can also choose to ignore the issue, but it is recommended to address the issues.

If you are notified of any issues, do these tasks:

- If any **Pending Operations** are identified, click the **Manage in Activities** link to go to the **Activities** > **Tasks** window (as displayed in the figure). You can **Discard** the pending operation, or you can wait for the process to complete. If you discard the pending operation, click **Recheck,** in the bottom-right corner of the window, to update the validation status.

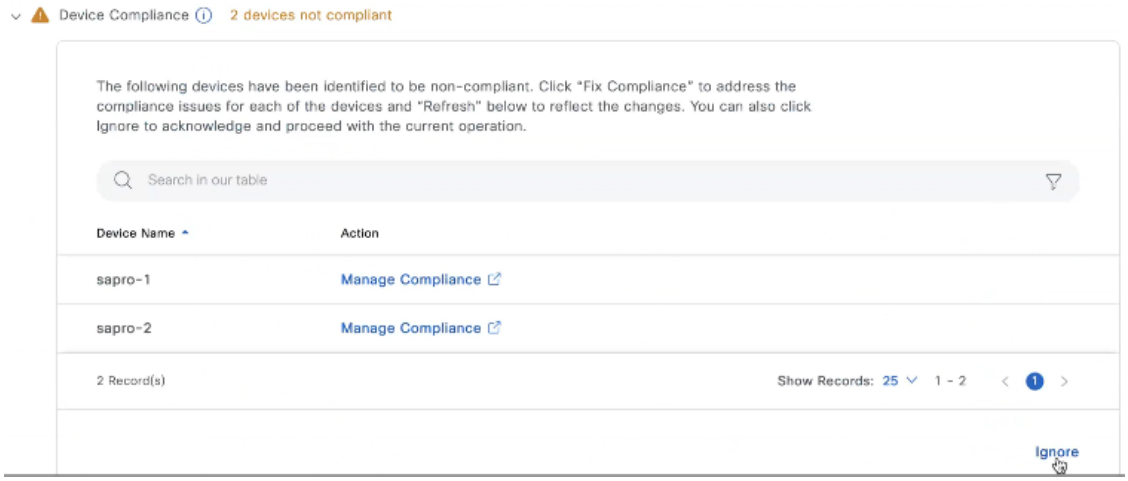


- If the **Device Compliance** check displays any noncompliant devices with links to each device's **Compliance Summary** window (as displayed in the figure), you must fix, acknowledge, or ignore the compliance issues to continue with provisioning.
  - To fix the issues, click **Manage Compliance** and then click **Fix Compliance** in the **Compliance Summary** window. For more information, see Fix compliance violations, on page 577.

Note The precheck checks for compliance violations (open and acknowledged) for only the Network Settings, Network Profiles, Fabric, Application Visibility, Umbrella, and Workflows tiles. It is not applicable for other categories available in compliance summary, as these categories are not affected by the provisioning workflow.

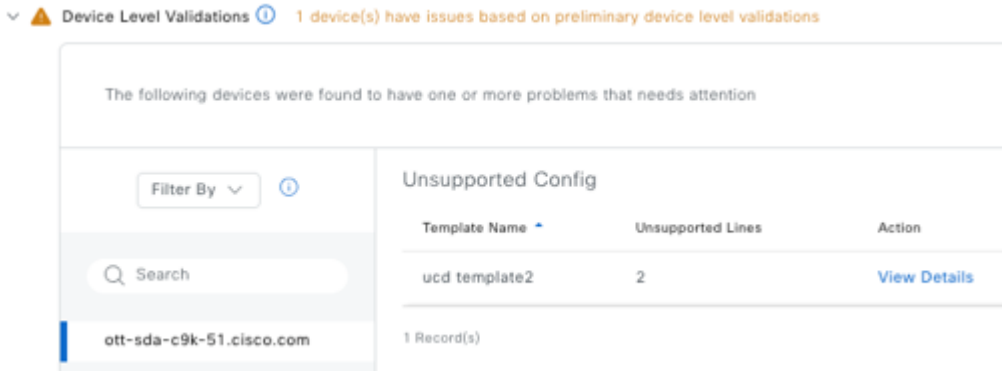
The acknowledged violations are also flagged during the precheck. This is to ensure that all compliance violations are checked before device provisioning.

- To ignore the issues, click **Ignore** in the **Device Compliance** area as shown in this figure.



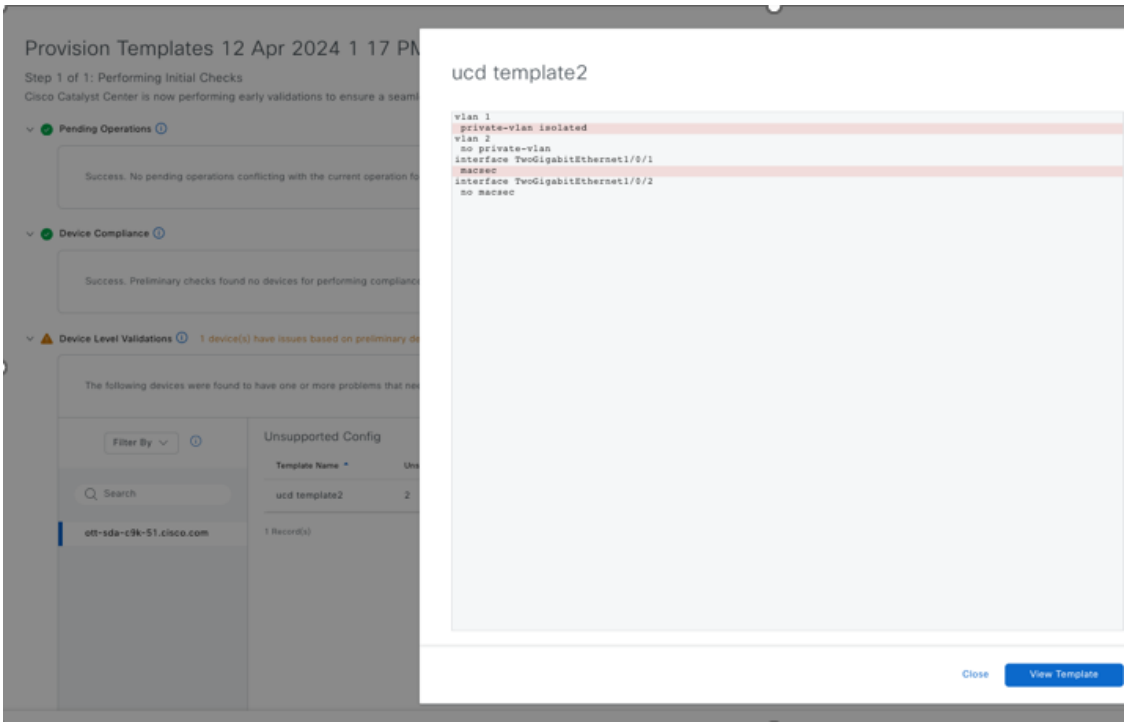
You must click **Recheck** in the bottom-right corner of the **Performing Validations** window to ensure the icon displays next to the prechecks. Then click **Next** to proceed to the next step in the provisioning workflow.

- The **Device Level Validations** check identifies the issues, including:
  - **Unsupported configurations used in the CLI template**: For a chosen device, the **Unsupported Lines** indicate the number of lines in a CLI template that have unsupported configuration.



Note This check is only applicable for fabric devices. Currently the check does not validate the CLI templates for non-fabric devices.

Click **View Details** to view the specific line with unsupported configuration highlighted, as shown in this image.



Hover your cursor over the highlighted CLI command to view the reason for which the line is highlighted.

To remove the unsupported configuration, click the **View Template** link. It will take you to the **CLI Template** window, where you can edit the template.

This table shows examples of unsupported configurations:

Item	Description
Macsec	Unsupported for fabric edge and extended nodes only.
Private-vlan	Unsupported on all fabric roles.
Flexlink + CLI (Rep segment)	Unsupported on fabric edge devices.

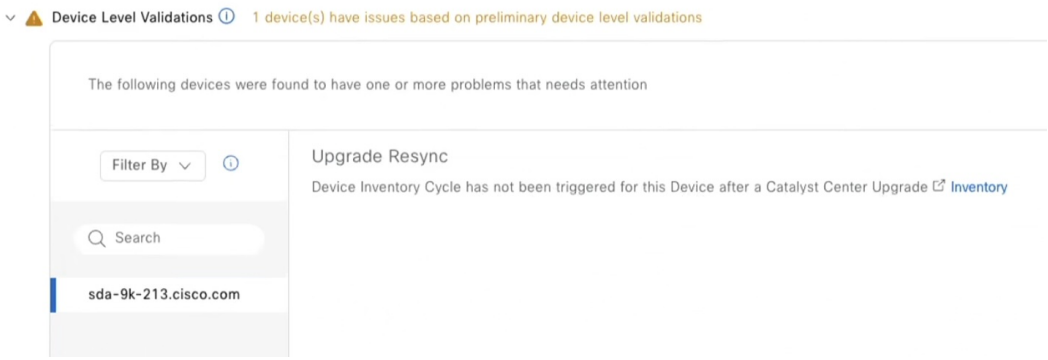
- After fixing the issues, click **Recheck** at the bottom-right corner of the **Device Level Validations** window to ensure the icon displays next to the prechecks. Then click **Next** to proceed to the next step in the provisioning workflow.

- If you wish to proceed without fixing the issues, you can click the **Ignore** button. It is not recommended to skip the issues.

- **Device is not resynchronized after an upgrade**: Lists one or more devices which have not been resynchronized after an upgrade. You must resynchronize the devices to proceed with the provisioning. Click the **Inventory** link to view the devices in the inventory and run the **Resync** operation.

Note

- Currently, this check is applicable for fabric devices only.
- For devices that are resynchronized after an upgrade but are unreachable or not in a managed state, an error message displays in the **Preview Configuration** window. You can choose to retry the resynchronization or continue to deploy the configurations that are generated.



After fixing the issues, click **Recheck** at the bottom-right corner of the **Device Level Validations** window to ensure the icon displays next to the prechecks. Then click **Next** to proceed to the next step in the provisioning workflow.

Note You must address the issues that are found during precheck to proceed with the deployment.

Replace a faulty device

The Return Material Authorization (RMA) workflow lets you replace failed devices quickly. RMA provides a common workflow to replace routers, switches, wireless controllers, and APs.

When using the RMA workflow with routers and switches, the software image, configuration, assurance data, and license are restored from the failed device to the replacement device. For wireless APs, the replacement device is assigned to the same site, which is provisioned with primary wireless controller, RF profile, and AP group settings, and placed on the same floor map location in Catalyst Center as the failed AP.

When replacing a member switch in Cisco switch stacks (hardware stacking), follow the same procedure. The active switch provides the software image and configuration to manage the replacement. Catalyst Center handles the full stack replacement.

Note

- You can also replace a faulty device using the **Replace Device** workflow. For more details, refer to Replace a device, on page 1407.
- Replacing a faulty device from the **Inventory** window streamlines the workflow, starting you on the **Choose Replacement Device** window. To replace a faulty device using the full Replace Device workflow, see Replace a device, on page 1407.
- Marking the device for replacement and replacing the device can be done at different times.

Before you begin

- Before marking the device for replacement, import the software image version of the faulty device in the image repository.
- Ensure that the faulty device is unreachable.
- Assign the faulty device to a user-defined site if the replacement device onboards to Catalyst Center through Plug and Play (PnP).
- Ensure that the replacement device is not in a provisioning state when you start the Replace Device workflow.
- For switch stack replacement, ensure that the faulty and replacement devices have the same number of stack members.
- Ensure the replacement wireless controller is not assigned to any site, not included in High Availability (HA) SSO, and not provisioned.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 From the **Inventory** window, mark the faulty device for replacement.

a) Check the check box of the faulty device that you want to replace.
b) From the **Actions** drop-down list, choose **Device Replacement** > **Mark Device for Replacement**.
c) In the **Mark for Replacement** dialog box, click **Mark** for confirmation.

Note To achieve seamless replacement of fabric devices, a DHCP server is configured on the neighbor device. This is required to assign an IP address to the replacement device for onboarding the device to Catalyst Center through PnP. This DHCP server is removed after successful replacement of the faulty device.

The latest configuration changes from the faulty device are pushed to the replaced device during the RMA workflow.

d) From the **Inventory** drop-down list, choose **Marked for Replacement**.

A list of devices that are marked for replacement displays.

e) (Optional) If you don't want to replace this device, check the check box of the device and choose **Actions** > **Unmark for Replacement**.

Step 3 (Optional) From the **Inventory** window, replace the faulty device.

a) Check the check box of the faulty device that you want to replace.

b) From the **Actions** drop-down list, choose **Device Replacement** > **Replace Device**.

c) In the **Choose Replacement Device** window, choose a replacement device from the **Plug and Play** tab or the **Inventory** tab and then click **Next**.

The **Plug and Play** tab shows the devices that are onboarded through PnP. The **Inventory** tab shows the devices that are onboarded through inventory or discovery.

For Cisco Catalyst 9800 Series Wireless Controllers and Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in SD-Access fabrics, you can select the **Plug and Play** tab to choose an unclaimed replacement device for zero-touch replacement.



Note If the faulty Cisco Catalyst 9800 Series Wireless Controller or embedded wireless controller is in an IPv6 fabric and runs a version earlier than Cisco IOS XE Release 26.1.1, the **Plug and Play** replacement device option is unavailable. Onboard the replacement device through inventory or discovery, then use the **Replace Device** workflow.

If the replacement device hasn't been onboarded through PnP, add it manually or automatically.

- Manual: Under the **Plug and Play** tab, click **Add Device**. Then in the **Add New Device** window, enter the serial number of the device and click **Add New Device**.
- Automatic: Under the **Plug and Play** tab, click **Sync with Smart Account**. Then, in the **Sync with Smart Account** window, click **Sync**.

d) For wireless controllers, in the **Configure replacement device** window, provide the required configuration details for replacement.

- If the faulty wireless controller has a master encryption key configured, enter the key in the **Master Encryption Configuration Key** field for the replacement wireless controller.



Note Encrypted passwords and keys cannot be restored without the correct master encryption key, which prevents access to the wireless controller and causes the RMA process to fail.

- Under **Configure HA**, select one of these options:
  - **Yes**: for replacing a faulty wireless controller High Availability (HA) pair with a new pair formed using the RMA workflow and two standalone wireless controllers.

    Complete the required configurations for both primary and secondary replacement wireless controllers.

Note For wireless controllers in a HA pair, use this workflow only if both devices in the pair are down. Do not use this workflow to replace a single faulty wireless controller within an active HA pair.

- **No**: for replacing a standalone wireless controller.

  Complete the required configurations for the replacement wireless controller.

To configure a replacement device, you can use the IPv4 address with its corresponding configurations, IPv6 address with its corresponding configurations, or both.

Note The IP address of the faulty wireless controller cannot be reused when claiming the replacement wireless controller through PnP.

Option	Description
Wireless Management IPv4	Enter a valid IPv4 address for the wireless management interface. **Note** • The wireless management IP address of the replacement wireless controller must be different from wireless management IP address of the faulty wireless controller. • To replace a faulty wireless controller HA pair with a new pair, the wireless management IP address of the primary and secondary wireless controllers must be different.
Subnet Mask	Choose a subnet mask for the IPv4 address.
Wireless Management IPv6	Enter a valid IPv6 address for the wireless management interface, if applicable. **Note** • The wireless management IP address of the replacement wireless controller must be different from wireless management IP address of the faulty wireless controller. • To replace a faulty wireless controller HA pair with a new pair, the wireless management IP address of the primary and secondary wireless controllers must be different.
Prefix Length	Choose an IPv6 prefix length.
Gateway IPv4	Enter the default gateway IPv4 address.
Gateway IPv6	Enter the default gateway IPv6 address.

Option	Description
VLAN ID	Enter the VLAN ID. The valid range is from 1 to 4094. **Note** The VLAN ID must be the same for both the faulty and the replacement wireless controller.
Interface Name	Enter the specific interface name used for wireless management.
Local Redundancy Management IP	Enter the local redundancy management IP address for the replacement wireless controller, if applicable. **Note** • Ensure that this IP address and the peer redundancy management IP address are not the same. • Ensure that this IP address is not assigned to any other network entity.
Select Secondary WLC	Choose a secondary wireless controller for HA, if applicable. **Note** To replace a faulty wireless controller HA pair with a new pair: • ensure that the wireless management IP address and subnet mask of the secondary wireless controller are in the same IP subnet as the wireless management IP address of the faulty wireless controller, • ensure that the wireless management VLAN of the secondary wireless controller matches the VLAN of the primary wireless controller, • Future wireless controllers cannot be selected as the primary or secondary wireless controllers. Only unclaimed, onboarded wireless controllers, and unprovisioned inventory-based wireless controllers can be selected.
Peer Redundancy Management IP	Enter the peer redundancy management IP address for the secondary wireless controller, if applicable. **Note** • Ensure that this IP address and the local redundancy management IP address are not the same. • Ensure that this IP address is not assigned to any other network entity.

e) On the **Summary** window, review the summarized details.

If necessary, click **Edit** to update the device type or faulty device details.

Note If Visibility and Control of Configurations is disabled, review the replacement device configuration by clicking **View** under **Replacement Device**.

f) In the **Schedule Replacement** window, schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 4 From the **Inventory** window, view the progress of the device replacement task as the device is replaced.

Alternatively, you can monitor the task from the **Tasks** window.

a. On the **Inventory** window, from the **Focus** drop-down list, choose **Device Replacement**.

b. In the **Replace Status** column, view the replacement status of the device.

If the device replacement is successful, the **Replaced** status is displayed.

If the device replacement fails and an error message displays, click the error link. Click **Retry** to retry the workflow with the same set of faulty and replacement devices.

Note The main inventory window displays the details of the new replacement device that has replaced the faulty device.

c. In the **Replace Status** column, click the status of the device to view more information in a slide-in pane.

For example, the slide-in pane displays these steps that the system follows to complete the task:

1. Run readiness checks for device replacement.
2. Claim the (PnP) replacement device.
3. Distribute and activate the software image to the replacement device.
4. Deploy licenses.
5. Provision VLAN configurations.
6. Provision startup configurations.
7. Reload the replacement device.
8. Check for reachability of the replacement device.
9. Deploy SNMPv3 credentials to the replacement device.
10. Synchronize the replacement device.

11. Remove the faulty device from CSSM.
12. Add the replacement device to CSSM.
13. Revoke and create the PKI certificate.
14. Update Cisco ISE.
15. Delete the faulty device.

What to do next

During wireless controller replacement, these files and configurations are not transferred to the replacement wireless controller:

- Custom web authentication bundles and NBAR protocol packs
- IP address SSH RSA keys or key pair names
- Custom trust points
- Regulatory activation file

After replacement, copy and reconfigure these settings manually on the replacement wireless controller.

Replace a faulty access point

Using the AP RMA feature, you can replace a faulty AP with a replacement AP available in the device inventory.

Before you begin

- The access point (AP) Return Material Authorization (RMA) feature supports only like-to-like replacement. The replacement AP must have the same model number and PID as the faulty AP.
- The replacement AP must have joined the same Cisco Wireless Controller as the faulty AP.
- A Cisco Mobility Express AP that acts as the wireless controller is not a candidate for the replacement AP.
- The software image version of the faulty AP must be imported in the image repository before marking the device for replacement.
- The faulty AP must be assigned to a site and provisioned in Catalyst Center.
- The replacement AP must not be in provisioning state while triggering the RMA workflow.
- The faulty AP must be in an unreachable state.
- You must have access to the site and devices where you want to perform the replacement.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Check the check box of the faulty AP that you want to replace.

Step 3 From the **Actions** drop-down list, choose **Device Replacement** > **Mark Device for Replacement**.

Step 4 In the **Mark for Replacement** dialog box, click **Mark** for confirmation.

If you decide that you don't want to replace this AP right now, you can unmark it for replacement and mark the correct faulty AP for replacement.

a. Check the check box of the AP that you don't want to replace.

b. From the **Actions** drop-down list, choose **Actions** > **Unmark for Replacement**.

c. Repeat Step 2, on page 212, Step 3, on page 212, and Step 4, on page 212 for the correct faulty AP.

Step 5 In the **Mark for Replacement** window, click the radio button next to the faulty device name.

Step 6 From the **Actions** drop-down list, choose **Replace Device**.

Step 7 In the **Replace Device** window, click **Start**.

Step 8 In the **Available Replacement Devices** table, click the radio button next to the replacement device name.

Step 9 Click **Next**.

Step 10 Review the replacement **Summary** and then click **Next**.

Step 11 In the **Schedule Replacement** window, choose a scheduling option, update the task name as necessary, and then click **Apply**.

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the deployment by setting the date, time, and time zone.

Step 12 Continue with the deployment based on the option that you chose.

- If you chose **Now**, click **Submit**.
- If you chose **Later**, click **Schedule**.

The task will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 13 From the **Inventory** window, monitor the task as the faulty AP is replaced.

Use this table to view AP replacement task details and retry a failed task.

If you want to...	Then...
view the progress of the task	**a.** On the **Inventory** window, from the **Focus** drop-down list, choose **Device Replacement**. **b.** In the **Replace Status** column, view the replacement status of the faulty AP as it's replaced. If the device replacement is successful, the **Replaced** status is displayed. **c.** Click the status of the faulty AP to view more information in a slide-in pane.
view the replacement history	**a.** On the **Inventory** window, from the **Focus** drop-down list, choose **Device Replacement**. **b.** From the **Actions** drop-down list, choose **Device Replacement** > **Replacement History**. The **Replacement History** slide-in pane lists the replaced devices in a tabular format. **c.** In the **Replace Status** column, click the status, such as **Replaced**, which indicates a successful device replacement. The **Replace Status** tab lists the steps that the system took to complete the task.
view the task failure reason	**a.** On the **Inventory** window, from the **Focus** drop-down list, choose **Device Replacement**. **b.** In the **Replace Status** column, view the AP replacement failure reason with the error message. You can either replace the faulty AP with another new AP or retry the failed replacement using the AP RMA Retry feature.
retry a failed AP replacement	**a.** On the **Inventory** window, from the **Focus** drop-down list, choose **Device Replacement**. **b.** In the **Replace Status** column, click the error message for that faulty AP and then click **Retry**.

Manage Out-of-band RMA device replacement

The term out-of-band replacement refers to manually replacing a device and transferring its configuration, image, and license to the new device, while bypassing the device replacement workflow on Catalyst Center.

The out-of-band replacement process results in a serial number conflict if the new device uses the same IP address as the old one. If the new device receives a different IP address, you must select the correct replacement device from a list.

To manage the out-of-band RMA device, complete these steps:

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Select the check box of the out-of-band RMA device that you want to manage in Catalyst Center.

Step 3 From the **Actions** drop-down list, choose **Device Replacement** > **Confirm Replacement (Out-of-Band)**.

After you confirm, the workflow maps the faulty device to the new device.

a. The workflow completes registration, synchronization, and certification tasks.

b. The inventory updates to show the new device with its serial number.

c. The replacement history displays details about the replacement.

Limitations of the RMA workflow in Catalyst Center

- RMA supports replacement of switches, routers, wireless controllers, and Cisco SD-Access devices, *except for*:
  - Cisco AireOS Wireless Controllers
  - Mobility Express devices
  - Chassis-based Nexus 7700 Series Switches
  - Switch stacks (SVL stacking)
- For Cisco SD-Access fabric devices, the RMA workflow supports only like-to-like device replacement. The replacement device must have the same model number and PID as the faulty device. Replacement with a different model number or PID is not supported.
- RMA supports devices with an external SCEP broker PKI certificate. The PKI certificate is created and authenticated for the replacement device during the RMA workflow. The PKI certificate of the replaced faulty device must be manually deleted from the certificate server.
- The RMA workflow supports device replacement only if:
  - Both the faulty and replacement devices have the same extension cards.
  - The number of ports in both devices does not vary because of the extension cards.
  - The faulty device is managed by Catalyst Center with a static IP. (RMA is not supported for devices that are managed by Catalyst Center with a DHCP IP, except extended node and AP in fabric.)

    - The replacement wireless controller is in Install Mode, as Software Image Management (SWIM) supports image updates only in this mode. If the replacement device is in Bundle Mode, image distribution and activation fail.

- Make sure that the replacement device is connected to the same port to which the faulty device was connected.
- The RMA workflow does not support shared WAN links—such as Metro-Ethernet—where multiple CDP neighbors are detected on the same interface.
- In Catalyst Center 2.3.7.4 and 2.3.7.5 only, fabric edge replacement does not support the DHCP server configuration in the neighbor device if the neighbor device is not part of the fabric. Because intermediate nodes are not part of the Cisco SD-Access fabric, the DHCP server with option 43 is not pushed.



Note This limitation is removed in Catalyst Center 2.3.7.6 and later.

- If the failed device is the only device in the fabric site (such as in a fabric-in-a-box deployment), Catalyst Center does not support configuring a DHCP server on a neighboring device, even if that device is also managed by Catalyst Center.
- Catalyst Center does not support legacy license deployment.

  The RMA workflow deregisters the faulty device from Cisco SSM and registers the replacement device with Cisco SSM.

    - If the software image installed on the faulty device is earlier than Cisco IOS XE 16.8, the **License Details** window does not display the Network and Feature License details and no warning message is displayed. Therefore, you should be aware of the legacy network license configured on the faulty device and manually apply the same legacy network license on the replacement device.
    - If the software image installed on the faulty device is Cisco IOS XE 16.8 or later, the **License Details** window displays details of the network license (for example, **Legacy** or **Network**) and the feature license (for example, IP Base, IP Service, or LAN Base). This warning message displays while marking the faulty device for replacement:

      ```
      Some of the faulty devices don't have a license. Please ensure your
      replacement device has the same Legacy license of the faulty device
      enabled.
      ```

    - If the legacy network licenses of the replacement and faulty devices do not match, this error message displays during the license deployment:

      ```
      Catalyst Center doesn't support legacy license deployment. So
      manually update the faulty device license on the replacement device
      and resync before proceeding.
      ```

- Catalyst Center supports PnP onboarding of the replacement device in a fabric network, *except when*:
    - The faulty device is connected to an uplink device using multiple interfaces.
    - LAN automation uses overlapping pools.
- If the replacement device onboards through the PnP-DHCP functionality, make sure that the device gets the same IP address after every reload and the lease timeout of DHCP is longer than two hours.

- In a fabric setup with Catalyst Center 9800 HA devices, if one of the HA devices goes down, you must complete these steps to replace it:

  1. From the **Inventory** window, resynchronize the HA device that failed. Catalyst Center shows the device as standalone; the standby has failed and has been removed.
  2. Set the priority for the devices. If you want the existing device to return as the active device after forming HA with the new device, ensure that the HA priority of the existing device is set to 2 (or the highest available priority value). You can configure the device priority from the web UI, under **Administration** > **Device** > **Redundancy**.

     Alternatively, you can enter this CLI command to configure the device priority:

     ```
     chassis <chassis_number> priority 2
     ```

     To view the chassis number and the current priority value, enter the `show chassis` EXEC command.

     If the priority is set to the default value of 1 on both devices, the device with the lower MAC address becomes the active device.
  3. Configure the chassis redundancy command on the new device using the same local and remote IP addresses that were used on the failed device. You can configure the chassis redundancy in either the web UI or the CLI.
  4. Reboot both devices to form the HA pair.
  5. After HA is up, resynchronize the devices in Catalyst Center. The **Inventory** window shows the new HA pair. Verify the serial numbers in the **Serial Number** column. For an HA pair, both the active and standby serial numbers are shown.

Reboot an access point

You can reboot one or more APs for troubleshooting and maintenance.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Check the check box of the APs that you want to reboot.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Reboot Device**.

Step 4 In the **Reboot Device** slide-in pane, select one of the scheduling options:

- **Now**: Reboots the devices immediately.
- **Later**: Schedules the reboot for a specific future time.
- **Recurring**: Schedules the reboot to execute N times.

Step 5 Expand **Selected Devices** to view the AP name and floor details of the reboot AP.

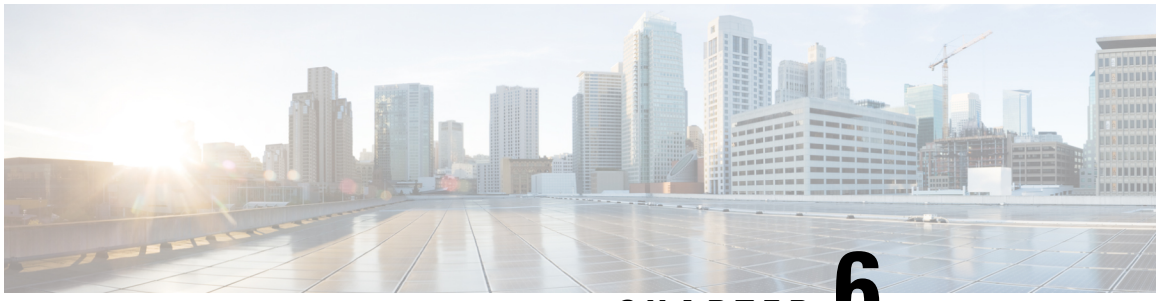
Step 6 Click **Reboot**.

After the Cisco Wireless Controller initiates the task of rebooting the selected APs, a `Reboot Initiated Successfully` message is displayed.

Step 7 In the **Task Submitted** dialog box, click the **Task** link.

This dialog box displays for a few seconds and then disappears. To navigate to the task, click the menu icon and choose **Activities** > **Tasks**.

Step 8 Click the task name to view the reboot initiation status.



CHAPTER 6

Display Your Network Topology

- About topology, on page 219
- Display the topology of areas, sites, buildings, and floors, on page 220
- Filter devices on a topology map, on page 220
- Display device information, on page 221
- Display link information, on page 223
- Pin devices to a topology map, on page 223
- Save a topology map layout, on page 224
- Open a topology map layout, on page 224
- Share a topology map layout, on page 225
- Export the topology layout, on page 225

About topology

The **Topology** window displays a graphical view of your network. Using the Discovery settings that you have configured, Catalyst Center discovers the devices in your network and assigns a device role to them. Based on the device role assigned during discovery (or manually changed in inventory), Catalyst Center creates a physical topology map with detailed device-level data.

Topology map

Using the topology map, you can do various tasks, including:

- Display the topology of a selected area, site, building, or floor.
- Display detailed device information.
- Display detailed link information.
- Filter devices based on a specific Layer 2 VLAN.
- Filter devices based on a Layer 3 protocol (such as Intermediate System - Intermediate System [IS-IS], Open Shortest Path First [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], or static routing).
- Filter devices with Virtual Routing and Forwarding (VRF) capability.
- Pin devices to the topology map.
- Save a topology map layout.

- Open a topology map layout.
- Export screen shots of the complete topology layout in SVG, PDF, and PNG format.

Display the topology of areas, sites, buildings, and floors

You can display the topology of an area, site, building, or floor.

Before you begin

- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.
- You must have defined a network hierarchy and provisioned devices to the buildings or floors within it.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 From the left hierarchy tree, select the area, site, building, or floor that you are interested in.

Step 3 In the top-right corner, use the toggle button () to switch between the Geographical map view and the Layer 2 map view.

The Geographical map view displays the sites. The nearer sites are grouped together and indicated with the number of sites in the group. The device health is indicated in different colors. Hover over the site to view the detailed device health.

Use the Search field in the top-right corner to find a building in the Geographical map view, and a device in the Layer 2 map view.

Note

- Click the legend icon (ⓘ) in the lower-right corner to open a legend that shows the available shortcut keys for the topology maps.
- Click the **Toggle Annotate** icon to draw annotations in the Layer 2 map. You can click the export icon to export the topology map along with the annotations.

Step 4 Click **Take a Tour** for information about the various options in the **Topology** window.

Filter devices on a topology map

You can filter devices based on one of these attributes:

- VRF
- VLAN

- Routing
- Tagging
- Redundancy

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 Click **Filter**.



Note If you are not able to view the **Filter**, click a site in the left tree view menu.

Step 3 Do one of these tasks:

- From the **VRF** drop-down list, choose the VRF that you want to view.
- From the **VLAN** drop-down list, choose the VLAN that you want to view.
- From the **Routing** drop-down list, choose the protocol that interests you.
- Click the **Redundancy** radio button, from the PRP drop-down list choose **Show Redbox, LAN A, LAN B** to view Parallel Redundancy Protocol (PRP) status.
- Click **View All Tags** and choose the tags you want to view. The devices associated with the selected tags is highlighted. If you want to create a new tag, do these steps:

a) Click **Create New Tag**.
b) Enter the **Tag Name**.
c) Click **Save**.

You can also associate a device with the tag by doing these steps:

a) Click the device.
b) Click **Tag Device**.
c) Select the tag to which you want to associate the device.
d) Click **Apply**.

Display device information

Catalyst Center allows you to display the device name, IP address, and other information about devices.

Note The device information that is accessible in the **Topology** window is also accessible in the **Device Inventory** window.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 In the topology area, hover your mouse over the device or device group that interests you.

Note A device group is labeled with the number and types of devices it contains. A blue arrow under a switch indicates that switch has a host. Click the blue arrow to view the host.

Step 4 Click **Display** and enable items to view additional device details. For more information, hover your mouse over the icon next to the items.

- **Device Health**: Displays the health of the devices.
- **Link Health**: Displays the health of the links between the devices.
- **License status**: Displays the license status of the device. Catalyst Center highlights a device if its license is about to expire and a warning icon appear next to it. Click the highlighted device to view its license details.
- **Device IP**: Displays device IP address under device label.
- **Device Suffixes**: Displays full name of the device, with its suffix.

Note
- Topology uses Link Layer Discovery Protocol (LLDP) to determine the neighbor devices when network devices are not configured with Cisco Discovery Protocol (CDP) in Catalyst Center.
- For third-party devices, only the added device icon displays, the links are not detected.

Display link information

Catalyst Center allows you to display information about the links in the topology map. For simple links, the display shows information for the single link. For aggregated links, the display shows a listing of all the underlying links. The information includes the interface name, its speed, and its IP address.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 Hover your cursor over the link that interests you.

Step 4 Click **Display** and enable **Link Health**.

A down link is shown in red. If you want to delete the link, select it and click **Delete**. To bring the link up:

a) Log in to the device.
b) Enable the interface.
c) Resynchronize the device on the Inventory page.

Note Topology uses Link Layer Discovery Protocol (LLDP) to determine the links for devices that are discovered using LLDP in Catalyst Center.

Pin devices to a topology map

Devices can be grouped or aggregated so that they take up less room on the map. However, at times, you might want to separate a device from its group. You can do this by pinning a device to the map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 Do one of these tasks:

- To pin a device, collapse the device group, click the collapsed group, and in the dialog box, click the pin icon to the left of the device name.
- To pin all the devices, collapse the device group, click the collapsed group, and, in the dialog box, click **Pin All**.

Note Double click the group to unpin the devices in the group.

Save a topology map layout

Catalyst Center has a Cisco-recommended topology layout that displays by default when you open the topology tool. You can customize multiple layouts and save them to view later. You can also set one of the layouts as the default to be displayed when you open the topology map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 Click **Custom View**.

Step 3 In the **Enter Focus Title** field, enter a name for your customized map.

Step 4 Click **Save**.

Step 5 (Optional) To set your customized map as the default, click **Custom View**, hover over the name of the custom map, and click ***** (default focus).

Open a topology map layout

You can open previously saved topology maps.

Before you begin

You should have saved topology map layouts.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.

Step 2 Click **Custom View**.

Step 3 Click the name of the map that you want to display.

Share a topology map layout

You can share a customized map with other users.

Before you begin

- You must have topology map layouts saved.
- You must have at least one topology view saved.

Procedure

Step 1 From the main menu, choose **Tools** > **Topology**.
Step 2 Click **Custom View**.
Step 3 Hover the cursor over the name of the custom map and click the **Share Focus** icon.
Step 4 In the confirmation window, click **Yes**.

Export the topology layout

You can export a snapshot of the full topology layout (up to a maximum of 16,384 pixels). The snapshot is downloaded as an SVG, PDF, or PNG file to your local machine.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

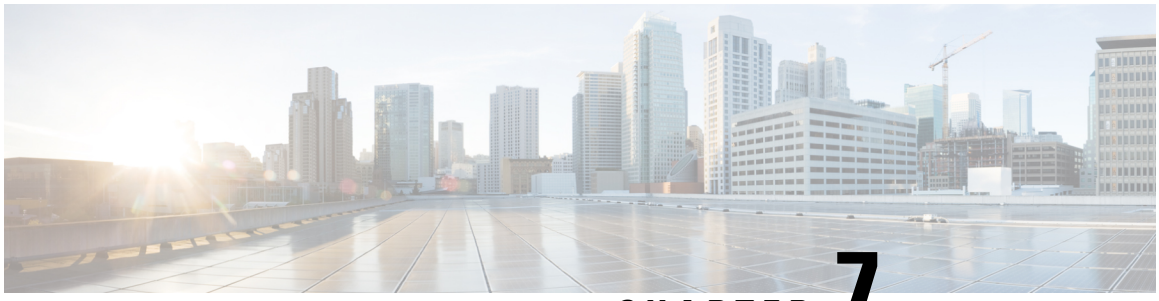
Step 1 From the main menu, choose **Tools** > **Topology**.
Step 2 Click  (this icon represents **Export Topology**).
Step 3 Select a file format and click **Export**.



PART III

Design Your Network

- Design the Network Hierarchy, on page 229
- Work with Wireless 2D and 3D Floor Maps, on page 247
- Configure Network Settings, on page 317
- Configure Network Profiles, on page 453



CHAPTER 7

Design the Network Hierarchy

- Network hierarchy, on page 229
- Design a new network hierarchy, on page 231
- Existing Cisco network hierarchies, on page 231
- Use an existing Ekahau network hierarchy, on page 235
- Export your network hierarchy from Catalyst Center, on page 238
- Search the network hierarchy, on page 240
- Create the network hierarchy, on page 240

Network hierarchy

You can create a network hierarchy that represents the geographical locations of your network.

Structure of a network hierarchy

The network hierarchy consists of sites. A site may refer to an area, building, floor, or an outdoor area. The placement of each site depends on network hierarchy rules. Refer to the figure and table to learn how to structure sites in your network hierarchy.

Figure 5: Network hierarchy

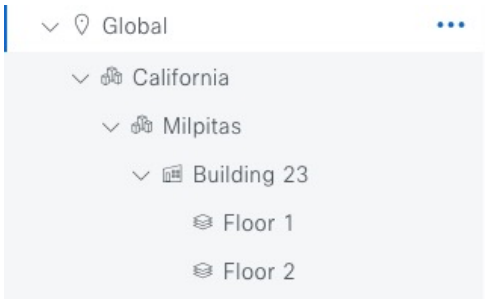


Table 40: Network hierarchy elements

Site types	Description	Rule
Global ( )	The default site element under which all other site elements reside.	Only areas and buildings can reside directly under **Global**.

Site types	Description	Rule
Areas ( )	Areas identify a geographic region. They group other areas, buildings, or both. Therefore, they do not have a physical address.	Areas can reside directly under **Global** or other areas.
Buildings ( )	Buildings can have physical addresses or latitude and longitude coordinates.	Buildings can reside directly under **Global** or areas. They cannot contain areas, but they can contain floors or outdoor areas.
Outdoor Areas ( )	Outdoor areas can be added with physical address or latitude and longitude coordinates and with or without an image map.	Outdoor areas can reside under **Global** or under areas or buildings. You can add them with or without maps. If you decide to use maps, you can manually create them or import them from files, such as DXF, DWG, JPG, GIF, PNG, or PDF file formats. Then you can position your wireless devices on the maps to visualize your wireless network coverage. You cannot add site elements under outdoor areas and cannot move an existing outdoor area from one site to another. **Note** You can add APs to an outdoor area, with a recommended maximum of 200 APs.
Floors ( )	Floors can be added to buildings with or without a background image that contains various building components, like walls and windows. Floor maps let you visualize wireless network coverage based on the position of your wireless devices on the floor map. You can manually create floor maps or add them from a background image, such as DXF, DWG, JPG, GIF, PNG, or PDF file formats.	Only floors reside under buildings. **Note** • You cannot move an existing floor to a different building. • You can change the site hierarchy for unprovisioned devices while preserving AP locations on floor maps.

Apply design settings to a site

The network hierarchy lets you apply design settings to a specific site. For example, you can apply design settings to an entire area or to a single floor.

Tip Naming hierarchical sites can help you identify where to apply design settings later.

Build your network hierarchy

To get started, build your network hierarchy using one of these methods:

- Create the network hierarchy. For more information, refer to Create the network hierarchy, on page 240.
- Import an existing network hierarchy from Cisco Prime Infrastructure or Ekahau Pro. For more information, refer to Existing Cisco network hierarchies, on page 231 or Use an existing Ekahau network hierarchy, on page 235.

Design a new network hierarchy

Use **Design** to create your network structure, network settings, and device type profiles that you can apply to devices throughout the network. If you do not have an existing infrastructure, use the **Design** workflow.

If you have an existing infrastructure, use the **Discovery** feature. For more information, refer to Discovery overview, on page 55.

Follow these steps to design a new network hierarchy:

Procedure

Step 1 Create your network hierarchy. For more information, refer to Create, edit, and delete a site, on page 240.

Step 2 Define global network settings. For more information, refer to Network settings overview, on page 317.

Step 3 Define network profiles. For more information, refer to Network profiles overview, on page 453.

Existing Cisco network hierarchies

An existing Cisco network hierarchy is a site structure that you can export from Cisco Prime Infrastructure, import into Catalyst Center, and use to preserve site hierarchy and map data.

If you have an existing network hierarchy in Cisco Prime Infrastructure, you can export it and then import it into Catalyst Center, saving time and effort when creating a new network hierarchy.

You can use this information to recreate your network hierarchy:

- **Site Hierarchy**: Your existing site hierarchy is downloaded as a CSV file. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.
- **Map Archive**: Map information is downloaded as a map archive TAR file. The map archive file contains data such as the date and time, number of floors, and APs. Depending on what you download, the map archive can also include map information, such as floor dimensions (length, width, and height) and details

about the APs and overlay objects that have been placed on the floor maps. You can also download calibration information, such as the RF attenuation model that has been applied to each floor.

You can base the map archive on the global hierarchy or on a single site, building, or floor:

- **Site**: The chosen site and all of its subsites, buildings, and floors are exported.
- **Building**: The chosen building and all of its floors are exported.
- **Floor**: The chosen floor is exported.



Note Catalyst Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Catalyst Center image. By default, FIPS mode is disabled.

FIPS mode affects the export and import of map archives.

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.
- Both encrypted and unencrypted map archives can be imported.

Export your site hierarchy from Cisco Prime Infrastructure

Use this task to export your site hierarchy from Cisco Prime Infrastructure as a CSV file. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

Site hierarchy export is supported in Cisco Prime Infrastructure, Release 3.2 and later.

Procedure

Step 1 In Cisco Prime Infrastructure, choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 In the **Device Groups** window, click **Export Groups**.

Step 3 In the **Export Groups** dialog box, select **APIC-EM**.

Step 4 To download the CSV file, click **OK**.

Export your map archive from Cisco Prime Infrastructure

Use this procedure to export map archive files from Cisco Prime Infrastructure and import them into Catalyst Center. Map archives contain map information, such as floor dimensions, and calibration information, such as the Radio Frequency (RF) attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

Procedure

Step 1 From the Cisco Prime Infrastructure GUI, choose **Maps** > **Wireless Maps** > **Site Maps (New)**.

Step 2 From the **Export** drop-down list, select **Map Archive**.

The **Export Map Archive** window opens, and the **Select Sites** window opens by default.

Step 3 Check the check box next to a specific site, campus, building, or floor that you want to export.

Alternatively, check the **Select All** check box to export all the maps.

Step 4 Select at least one of these options:

- **Map Information**: Click **On** to export floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps.
- **Calibration Information**: Click **On** to export the RF attenuation model that has been applied to each floor. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must re-enter the calibration details manually.

  If you include calibration information, you also need to specify whether to include information for the selected maps or all the information.

  - **Calibration Information for selected maps**: Calibration information for the selected site maps is exported.
  - **All Calibration Information**: Calibration information for the selected map and any additional calibration information that is available in the system is exported.

Step 5 Click **Generate Map Archive**.

This message shows the progress of the operation:

```
Exporting data is in progress
```

A TAR file is created and saved to your local machine.

Step 6 Click **Done**.

Import your site hierarchy to Catalyst Center

Use this procedure to import a site hierarchy that you exported from Cisco Prime Infrastructure as a CSV file. For information about exporting the site hierarchy, refer to Export your site hierarchy from Cisco Prime Infrastructure, on page 232.

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your Catalyst Center inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- If you manually created sites in Catalyst Center that are present in Cisco Prime Infrastructure, you must remove them from Catalyst Center before you can import them.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the map toolbar, click **Import** and select **Import Sites**.

Step 3 In the dialog box, select one of these options:

- **Merge with Existing Sites**: The imported site information is combined with the existing site information.
- **Overwrite Existing Sites**: If the same site already exists in Catalyst Center, the existing site information is overwritten with the imported site information.

Step 4 In the dialog box, drag and drop your CSV file into the download area.

To use the file picker instead, you can click **Choose a file**, navigate to where your CSV file is located, and then click **Import**.

Note If you do not have a CSV file, click **CSV template** to download a CSV file that you can edit and upload.

Import your map archive to Catalyst Center

Use this task to import a map archive TAR file that you exported earlier into Catalyst Center. For example, you can upload the TAR file that you exported from Cisco Prime Infrastructure.

Note Catalyst Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Catalyst Center image. By default, FIPS mode is disabled.

For information about exporting a map archive, refer to Export your map archive from Cisco Prime Infrastructure, on page 233.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the map toolbar, click **Import** and select **Import Floor Maps**.

Step 3 In the **Import Floor Maps** dialog box, drag and drop the map archive file.

Step 4 Click **Import**.

The map archive file is imported.

Use an existing Ekahau network hierarchy

The Ekahau Pro tool lets you create a complete network plan for your enterprise, including floor layout, AP locations, and obstacles. After creating the floor layout, you can export the simulated network plan as an Ekahau project file. You can also export the real-world site survey data into a format that Catalyst Center can use.

Export the Ekahau project from Catalyst Center

To augment the preconfigured working floors, the Catalyst Center allows you to export the working floors from Catalyst Center as an Ekahau project and import the project into the Ekahau Pro Tool.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

A world map displays in the right pane.

Step 2 In the left pane, select the site, building, or floor.

Step 3 To export a complete network map as an Ekahau project, from the **Export** drop-down list, select **Export Floor Maps**.

To export an Ekahau project of a site, building, or floor map, from the left pane, hover over the ellipsis ••• next to the site, building, or floor and select **Export Floor Maps**.

The **Export Floor Maps** dialog box is displayed.

Step 4 In the **Export Floor Maps** dialog box, select the **Ekahau Project** export format.

Step 5 Click **Export**.

An ESX file is created and saved to your computer.

Step 6 Import the ESX file into the Ekahau Pro tool, augment the floor, and save the file.

Step 7 Import the Ekahau project into the Catalyst Center under the site. For more information, see Import an Ekahau project to Catalyst Center, on page 236.

Import an Ekahau project to Catalyst Center

Before you begin

Importing an Ekahau Cloud project can fail if the project has local changes (such as removing an AP or wall), that are out-of-sync with the Ekahau Cloud project. To avoid this situation, make sure to synchronize any local changes to the Ekahau Cloud before importing the Ekahau Cloud project to Catalyst Center.

For the Ekahau versions that Catalyst Center supports, see the Compatibility Matrix. Ekahau releases new versions periodically. For information about importing a later version than Ekahau 11.0.2, see the Ekahau support article titled How to import Ekahau data into the Cisco Catalyst Center.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 Add the sites, buildings, and floors that you need in the network hierarchy.

Note For more information, see Create, edit, and delete a site, on page 240, Add, edit, and delete a building, on page 242, and Add, edit, and delete a floor, on page 242.

While adding floors, make sure that you create floors with the same name given in the Ekahau project.

Step 3 In the left pane, hover your cursor over the ellipsis ••• icon next to the site where you want to import the Ekahau project and select **Import Ekahau Project**.

The **Import Ekahau Project** dialog box appears.

Step 4 Drag and drop the ESX file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the ESX file.

Note To import buildings, add coordinates to them in the Ekahau project. You can add coordinates in Ekahau Pro. After successfully importing an Ekahau Project, each planned AP is mapped to an existing real AP in the inventory using the AP name. The planned AP is displayed with an icon **P** on the floor map. For example, if the name of the planned AP is SJC01-02-AP-B-1, the import process searches for the real AP with the same name.

Step 5 If an AP is not found in the inventory and remains unmapped, the planned AP is retained on the floor.

To see the reason for the mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.

These attempts are made to map the planned APs to real APs:

- If the newly discovered APs match the planned AP, the planned AP is replaced with the discovered real AP.
- If a planned AP remains unmapped, you can manually replace the planned AP with the real AP, providing reasons for the failure.

Step 6 To manually assign the planned AP to a real AP, hover your cursor over the planned AP icon on the floor map, and click **Assign** > **Assign**.

The **Assign Planned APs** panel appears.

Step 7 In the **Assign Planned APs** panel, map the planned AP to a real AP by AP name, AP type, or All APs.

Step 8 Click the radio button next to the **AP Name**, and click **Assign** to manually assign the planned AP.

Step 9 Click **Save**.

Import an Ekahau site survey to Catalyst Center

To create your network hierarchy, you can upload an Ekahau site survey file and an AP mapping file (in CSV format).

The Ekahau site survey only contains the floor map with the APs known by name and position on the map. By default the AP model might not be set in the Ekahau site survey. A prerequisite of importing to Catalyst Center is to open the project in Ekahau and configure the AP models using Ekahau-allowed model names, for example, *Cisco C9130i* for the Catalyst Center 9130 AP.

Because the Ekahau site survey does not provide Catalyst Center with any information about the radios of each AP, the AP mapping file augments the Ekahau site survey with this information. The AP mapping file is limited in that you can only provide the desired AP mapping by AP model, not by AP name. So, if you have multiple APs of the same type but different antenna configurations, only one antenna configuration can be applied to all APs of that type within the project.

For each AP in the AP mapping file, you define the model number followed by the configuration of each antenna:

```
model,antennaName0,antennaAzimuth0,antennaElevation0,antennaName1,antennaAzimuth1,antennaElevation1
```

For example, this AP mapping file defines the configuration of a Catalyst 9130I with two antennas:

```
AP9130I,Internal-9130-2.4GHz,90d,0d,Internal-9130-5GHz,90d,0d
```

The model attribute must be the same as the equivalent planned AP model in the Catalyst Center GUI, for example, AP9130I for the Catalyst Center 9130 AP. Similarly, the *antennaName* attributes must also be the same names found and supported in the Catalyst Center GUI. If the AP has three or more radios, you can continue the *n*-based numbering pattern of the *antennaName*, *antennaAzimuth*, and *antennaElevation* parameters to define the antenna information for each radio by slot number supported by that AP model.

Catalyst Center includes a CSV template file that you can download and edit to define the required AP antenna information.

Figure 6: Fields and defaults contained in the CSV template file

	A	B	C	D	E	F	G	H	I	J
1	model	antennaName0	antennaAzimuth0	antennaElevation0	antennaName1	antennaAzimuth1	antennaElevation1	antennaName2	antennaAzimuth2	antennaElevation2
2	AP2700I	Internal-2700-5GHz	90d	0d	Internal-2700-2.4GHz	90d	0d			
3	AP1850I	Internal-1850-5GHz	90d	0d	Internal-1850-2.4GHz	90d	0d			
4	AP3800E	AIR-ANT2524DB-R-5GHz	179.9543762d	0d	AIR-ANT2524DB-R-2.4GHz	179.9543762d	0d			
5										

If an AP isn't in the Catalyst Center device inventory, it's imported as a planned AP. However, you can use a naming convention so that when you add an AP to the device inventory, Catalyst Center can automatically convert it to an actual AP.

The naming convention is AP, followed by the last four digits of the AP's MAC address, for example, AP-c4:e0. Using this information, Catalyst Center attempts to match the provided digits with the last four digits of an

AP's Ethernet MAC or radio MAC address. If this information isn't available or a match is unsuccessful, Catalyst Center attempts to match AP names.

Before you begin

- Open the project in Ekahau and configure the AP models using Ekahau-allowed model names, for example, *Cisco C9130i* for the Catalyst Center 9130 AP.
- Create an AP mapping file (CSV format) to provide Catalyst Center with information about the radios of each AP model that is being used.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 Click **Add Site** > **Add Area**.

Alternatively, you can hover over the ellipsis ••• next to the parent site or **Global** in the left pane, and select **Add Area**. For more information, see Create, edit, and delete a site, on page 240.

Step 3 In the left pane, hover your cursor over the ellipsis ••• icon next to the site you just created and select **Import Ekahau Survey**.

Step 4 In the **Import Ekahau Survey** dialog box, drag and drop the Ekahau Survey file into the **Ekahau Survey** box, or click the **Choose a file** link and browse to the ESX file.

Step 5 Drag and drop the CSV file into the **AP Mapping CSV** box, or click the **Choose a file** link and browse to the CSV file.

Note If you do not have a CSV file, click **Download AP Mapping Template** to download a CSV file that you can edit and upload.

Step 6 Click **Import**.

After the files are successfully uploaded, a success message appears.

Step 7 Click **View Hierarchy** and navigate to the floors to verify that the devices have been imported and positioned properly.

Hover the cursor over a device to view its details.

Export your network hierarchy from Catalyst Center

You can export a site hierarchy to a CSV file. You can also export a complete network map (global hierarchy) or the hierarchy of a site, building, or floor. You can choose either a Cisco Prime Infrastructure or Ekahau Pro format. Exporting your network hierarchy in these formats lets you work on your network hierarchy in these tools.

Export your site hierarchy from Catalyst Center

You can export a site hierarchy to a CSV file. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the map toolbar, click **Export** and choose **Export Sites**.

Step 3 In the **Export Sites** dialog box, click **OK**.

Export your map archive from Catalyst Center

You can export a complete network map (global hierarchy) or the hierarchy of a site, building, or floor to either a Cisco Prime Infrastructure or Ekahau Pro format. You can export up to 500 floors.

Note Catalyst Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Catalyst Center image. By default, FIPS mode is disabled.

FIPS mode affects the export and import of map archives in these ways:

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.
- Both encrypted and unencrypted map archives can be imported.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 To export the complete network map, from the map toolbar, click **Export** and choose **Export Floor Maps**.

To export the hierarchy of a site, building, or floor map, from the left pane, hover over the ellipsis (•••) next to a site, building, or floor and choose **Export Floor Maps**.

The information that is exported depends on what you choose:

- **Site**: The chosen site and all of its subsites, buildings, and floors are exported.

- **Building**: The chosen building and all of its floors are exported.
- **Floor**: The chosen floor is exported.

Step 3 In the **Export Floor Maps** dialog box, click either the **Ekahau Project** or the **Prime** radio button.

Step 4 Click **Export**.

Search the network hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

Procedure

Step 1 To search the hierarchy, from the **Search Hierarchy** search field in the left pane, enter either the partial or full name of the site, building, or floor name that you want to find.

The hierarchy is filtered based on the text you enter in the search field.

Step 2 To search the hierarchy by **Site Name** and **Site Type** filter criteria, click the filter icon in the **Search Hierarchy** search field and do these steps:

a. In the **Site Name** field, enter the name of the site that you want to search.

b. Check the **Include Address for all Building** check box to include the address of all buildings in the search result.

c. In the **Site Type** area, check the check boxes next to **Area**, **Building**, or **Floor** that you want to include in the filter criteria.

d. Click **Search**.

The hierarchy is filtered based on the filter criteria.

e. To exclude the search criteria in the left pane, click the cross-mark next to each criterion.

Create the network hierarchy

Create the network hierarchy by creating new areas, buildings, and floors.

Create, edit, and delete a site

Catalyst Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can

add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

A world map appears in the right pane.

Step 2 From this window, you can add, edit, and delete sites. See this table for details.

Action	Steps
Add a site.	**a.** From the map toolbar, click **+ Add Site** > **Add Area**. Alternatively, you can hover your cursor over the ellipsis ••• next to the parent site in the left pane, and select **Add Area**. **b.** In the **Area Name** field, enter the site name. The **Area Name** field has restrictions, including: • The area name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. **c.** From the **Parent** drop-down list, select a parent node. **Global** is the default parent node. **d.** Click **Add**.
Edit a site.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the site and select **Edit Area**. **b.** In the **Edit Area** dialog box, make the necessary edits. **c.** Click **Update**.
Delete a site.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the site and select **Delete Area**. **b.** Click **OK**.

Note After you create the network hierarchy, you can move the sites between different parent sites only when:

- The new parent site has the same network settings as the current parent site.
- The new parent site has the same network profiles assigned as the site being moved.

Add, edit, and delete a building

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a building. See this table for details.

Action	Steps
Add a building.	**a.** In the **Network Hierarchy** window, click **+Add Site** > **Add Building**. Alternatively, you can hover your cursor over the ellipsis ••• next to the parent site in the left pane, and select **Add Building**. **b.** In the **Add Building** dialog box, add the building details. The **Building Name** field has restrictions, including: • The building name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. You can enter the address in the field or click the map. Adding an address causes the **Longitude** and **Latitude** coordinate fields to be automatically populated. These coordinates correspond to the northwest corner of the building and are used by location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), if they are integrated with Catalyst Center. **c.** Click **Add**.
Edit a building.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the site and select **Edit Building**. **b.** In the **Edit Building** dialog box, make the necessary edits. **c.** Click **Update**.
Delete a building.	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the building and select **Delete Building**. **b.** Click **OK**.

Add, edit, and delete a floor

After you add a building, you can add floors to it. You can add a basic floor that doesn't have a floor map and add the floor map later, or you can add a floor and include a floor map at the same time.

To add a basic floor to a building, use this procedure.

To add a floor and a floor map at the same time, see one of these topics:

- Add a floor with a CAD map file, on page 250
- Add a floor with a non-CAD map file, on page 251
- Import an Ekahau project to Catalyst Center, on page 236

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a floor. See this table for details.

Action	Steps
Add a basic floor	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the desired building and select **Add Floor**. **b.** In the **Floor Name** field, enter a name for the floor. The **Floor Name** field has restrictions, including: • The floor name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. **c.** In the **Global Unit System** area, select **Feet** or **Meters**. When the floor is added, all the floors across all the sites sync to display all measurements in your chosen unit system. To update the global unit system, see 2D map view options, on page 289. **d.** If you have wireless devices, for the **Type (RF Model)** drop-down list, select the RF model to apply to the floor. The RF model determines how the RF is calculated when computing 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. **e.** Configure the **Floor Number**, **Floor Type** and **Thickness** fields. The floor type and thickness are used when calculating a heatmap for wireless devices. **f.** Skip uploading a floor map image in **Floor Image** area. **g.** Configure map dimensions in the **Width**, **Length**, and **Height** fields. **h.** Click **Add**.
Edit a floor	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the floor and select **Edit Floor**. **b.** In the **Edit Floor** dialog box, make the necessary changes. **c.** Click **Update** to save the changes.

Action	Steps
Delete a floor	**a.** In the left pane, hover your cursor over the ellipsis ••• next to the floor and select **Delete Floor**. **b.** Click **OK**.

Add, edit, and delete an outdoor area

You can add outdoor areas under the global site, an area, or a building. Use this procedure to add, update, or delete an outdoor area.

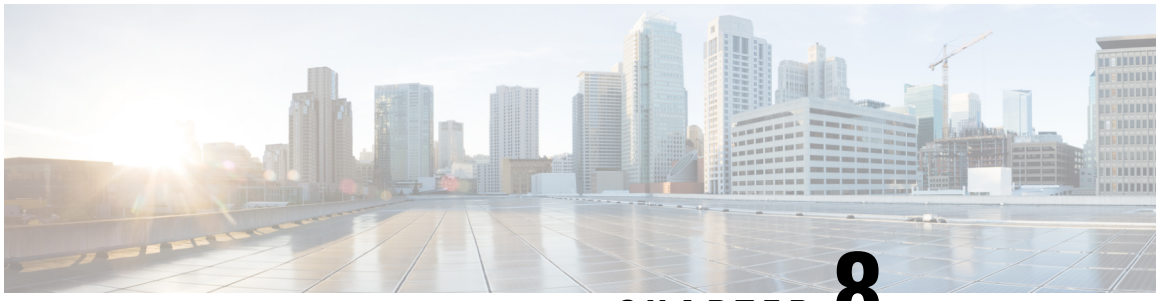
Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**

Step 2 From this window, you can add, edit, and delete an outdoor area. See this table for details.

Action	Steps
Add an outdoor area	**a.** In the **Network Hierarchy** window, click **+Add Site** > **Add Outdoor Area**. Alternatively, you can hover your cursor over the ellipsis icon (•••) next to the parent site in the left pane, and select **Add Outdoor Area**. **b.** In the **Outdoor Area Name** field, add a name for the outdoor area. The **Outdoor Area Name** field has restrictions, including: • The name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. **c.** In the **Address** field, enter the address or click on a location in the map. When you add an address, the **Longitude** and **Latitude** coordinate fields are automatically populated. **d.** In the **Global Unit System** area, select **Feet** or **Meters**. **e.** In the **Type (RF Model)** drop-down list, select the RF model to apply to the outdoor area. **f.** In the **Outdoor Area Image** area, upload a map image for the outdoor area. **g.** Configure the map's dimensions in the **Width**, **Length**, and **Height** fields. **h.** Click **Add**.

Action	Steps
Edit an outdoor area	**a.** In the left pane, hover your cursor over the ellipsis icon (•••) next to the outdoor area and select **Edit Outdoor Area**. **b.** In the **Edit Outdoor Area** dialog box, make the necessary edits. **c.** Click **Update**.
Delete an outdoor area	**a.** In the left pane, hover your cursor over the ellipsis icon (•••) next to the outdoor area and select **Delete Outdoor Area**. **b.** Click **OK**.



CHAPTER 8

Work with Wireless 2D and 3D Floor Maps

- Floor maps overview, on page 247
- Heatmap overview, on page 247
- Add a floor with a map file, on page 248
- Work with 2D maps, on page 254
- Work with 3D maps, on page 297

Floor maps overview

There are several reasons to add floors with floor maps. One reason is to see your wireless network the way it exists today. Another reason is to help you plan and visualize future changes.

You can visualize your wireless network by creating or importing a floor map that contains various building components, like walls and windows, and then positioning your wireless devices on it.

Interactive planning helps you plan a floor layout by drawing planned, or hypothetical, APs and obstacles with a raster image or a CAD floor plan as the backdrop. You can export the floor map as a PDF and share it with the technicians who are mounting the APs. The floor drawing helps the technicians to visualize the floor layout and the exact AP mount locations.

With interactive floor planning, you can:

- Create a floor layout with a raster or CAD floor plan as the canvas.
- Place the planned APs or hypothetical APs on the floor map based on the signal coverage requirement. These hypothetical APs or planned APs are not yet installed or discovered by Catalyst Center.
- Assign the antenna type and orientation.
- Draw obstacles, such as walls and shelving on the floor, that impact the signal attenuation.
- Plan all APs in sequence.
- Export the floor map as a PDF.

Heatmap overview

A heatmap is a visual representation of the Radio Frequency (RF) signal coverage of the wireless network devices in a particular area. In Catalyst Center, you can generate a heatmap on a per floor basis by creating

or importing a floor map that contains various building components, like walls and windows, and then positioning your wireless devices on it.

Using the floor map, Catalyst Center computes 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. For 2D wireless maps, the heatmap is computed at height of 3 feet from the floor, while in 3D wireless maps, the heatmap is computed using the entire volume of the floor (from floor-to-ceiling). For this reason, using 3D wireless maps is especially useful for computing wireless coverage in high-ceiling environments, like warehouses.

In addition, the 3D wireless heatmap can compute the effect of a floor's signal coverage on its neighboring floors. Neighboring floors are the two floors directly above and below the selected floor. Neighboring floors are configurable, meaning you can choose which neighboring floors you want to use in a heatmap computation. (See **Contributing Floors** in 3D map view options, on page 302.) In this way, you can detect, visualize, and analyze the impact of a floor's signal coverage on other floors. For example, you might have clients on the first floor who are connecting with APs on the second floor, or clients might be competing for signal on the same channel (called cochannel interference). In some cases, this might be an intentional design. However, if this design isn't intentional, you can take steps to change it.

The legacy heatmap generator is still available to be used. However, we recommend that you use the enhanced 3D-computed heatmap generator for both 2D and 3D heatmaps, because it can generate heatmaps much faster.

3D-computed heatmap generator

The 3D-computed heatmap generator, which is enabled by default, offers several advantages over the legacy heatmap generator. It uses the specialized graphics processing unit (GPU) to accelerate graphics rendering. Therefore, it can generate heatmaps substantially faster than the legacy heatmap generator. In addition, you can set a limit to the number of walls that are included in a heatmap computation, which also helps to enhance processing speed.

The 3D-computed heatmap generator automatically removes small obstructions (under 0.75 ft) and the second sides of the walls, leaving only one side per wall. (Catalyst Center applies an attenuation value for each wall, not for each side of a wall.)

Legacy heatmap generator

The legacy (server-based) heatmap generator is still available to be used. However, we recommend that you use the enhanced 3D-computed heatmap for 2D heatmaps because performance and accuracy are much better.

The legacy server-based heatmap generator has a limit on the number of walls that can used to compute 2D and 3D heatmaps. The maximum number of walls for a 2D heatmap is 300, after optimization. If your CAD file contains more, Catalyst Center alerts you and preserves the 300 most relevant walls (based on the length of the wall multiplied by its attenuation). The maximum number of walls for a 3D heatmap is 3000, after optimization. If your CAD file contains more, Catalyst Center alerts you and preserves the 3000 most relevant walls (based on the length of the wall multiplied by its attenuation).

Although the 3D-computed heatmap generator is enabled by default, you can disable it and use the legacy heatmap generator instead.

Add a floor with a map file

When you create a floor, you can include a floor map at the same time. These topics help you understand the different floor creation methods depending on the floor map file type that you use. Procedures for each method are also provided.

Floor map creation methods

To view a wireless map, first you need to create or import a floor map:

- **Create a Floor Map**: To create a floor map from scratch, you need to add the floor elements manually. The floor elements, like walls, windows, shelving, and so on, are displayed in the wireless map and used for heatmap computations. For details, see 2D floor map devices and overlay objects, on page 255.
- **Import a CAD file**: When you use a CAD file (DXF or DWG file type) to import a floor map, Catalyst Center converts the CAD layers into the floor elements (walls, windows, shelving, and so on) that you specify. The floor elements are displayed in the wireless map and are used for heatmap computations.

  Previously, Catalyst Center didn't limit the number of walls that could be imported from a CAD file. Now, however, Catalyst Center allows you to set a limit. The fewer walls you import, the less time it takes for the heatmap to be computed. For more information about heatmap generation, see Heatmap overview, on page 247.

  When deciding which layers and elements to import, focus on obstacles that create the most signal attenuation. In principle, the longer, thicker, and denser a wall is, the higher its attenuation. Low walls, like cubicles, and narrow walls, like columns, have low attenuation and have little effect on the heatmap. However, even if a material of an obstacle is dense, the attenuation might not be significant if the signal can radiate around it. If you're not interested in the coverage outside of a building, don't include external walls or windows. Doing so provides better 3D visualization of the inside of the building.

  If your CAD file doesn't have walls in specific layers but has walls mixed with other elements, don't select them for import. You can add walls manually later. For information, see Add, edit, and remove walls, on page 280.

  Block inserts and proxy entities can't be imported. Imported layers must contain only native elements like lines, polylines, arcs, and so on.

  For the procedure, see Add a floor with a CAD map file, on page 250.
- **Import a non-CAD image file**: You can use JPG, GIF, PNG, or PDF files to import the floor plan. Typically, this type of file is used to create 2D floor maps. However, you need to manually create the floor elements, such as the walls and shelving, for them to be represented in the wireless map. For the procedure, see Add a floor with a non-CAD map file, on page 251.
- **Import a Ekahau Pro Project plan**: You can import Ekahau project data, such as the obstacles, APs, and more, to create a wireless map. For the procedure, see Import an Ekahau project to Catalyst Center, on page 236.

Guidelines for image files to use in maps

Follow these guidelines to use map image files:

- Use a graphical application that can save the map image files to any of these formats: JPG, GIF, PNG, PDF, DXF, and DWG.
- Map image files can be of any size. Catalyst Center imports the full definition of the original images to its database, but during display, it automatically resizes them to fit the workspace.
- Obtain the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.

- Avoid using floor map images with rotation metadata, because the images might not render correctly when synced to CMX or Cisco Spaces. Although the floor map images might be in formats that are supported by Catalyst Center, the ways in which certain tools add the metadata can be rendered differently. For example, an image file with rotation metadata that is opened in three different applications might render horizontally in two applications and vertically in the other.

Add a floor with a CAD map file

You can use CAD files (DXF or DWG file types) to create a floor map.

For 2D floor maps, you must choose the CAD layers that you want to be used in the 2D view. For 3D floor maps, Catalyst Center converts the CAD layers you choose into the floor elements that you define. You can define floor elements as walls, shelving, windows, obstacles, and so on.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, hover your cursor over the ellipsis ••• next to the building and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Step 4 From the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 5 Drag and drop the CAD file (the DXF or DWG file type) to the **Floor Image** area.

When importing a CAD file, Catalyst Center will only import entities of these types:

- Lines, open polylines, and closed polygons: LINE, LWPOLYLINE, POLYLINE, and SOLID
- Radius-based: ARC, CIRCLE, ELLIPSE (including arcs of ellipse)
- Other geometry elements: SPLINE
- Texts: ATTRIB, MTEXT, TEXT
- Block insertions (normally used for furniture): INSERT

Note By default, overlays are not displayed after you import a map. So, after you import a floor plan, make sure that you enable the overlay visibility. From the map toolbar, click **View Options**. From the right pane, expand **Overlay Objects** and click the toggle button for each object you want to display.

Step 6 In the **Floormap** window, choose the CAD layers that you want to include in the floor map:

a) In the **2D** column, check the check boxes corresponding to the CAD layers that you want in the 2D floor map.

Tip If some elements aren't displayed on the map (even when the **2D** check boxes are checked for the corresponding CAD layers), go to AutoCAD, open the required CAD file, select all the elements in the required layers, run the **Explode** command, and save it as a new DWG file. This action converts unsupported wrapper entities, like group and proxy entities, to entities that Catalyst Center can read. Then close the **Floormap** window and upload the updated CAD file (see Step 5, on page 250).

b) In the **Wall/Shelving Type** column, click the drop-down and, for each CAD layer that you want converted, choose the wall or shelving type that you want the CAD layer converted into.

Each wall or shelving type has a decibel (dB) value associated with it. This dB value is used to compute signal attenuation in the heatmap. For more information, see Floor map creation methods, on page 249.

After a wall or shelving type is selected, the **Counter** column is updated with the number of units detected in the CAD file and the **Total Selected Walls Counter** is incremented. If the total number of selected walls exceeds the import walls limit, you have three options to proceed:

- Add the floormap with the current number of walls. In this case, Catalyst Center imports only the most relevant walls (equal to the import walls limit).
- Increase the import walls limit. Keep in mind that the more walls you import, the longer it takes for the heatmap to be computed.
- Decrease the total number of selected walls to a number that doesn't exceed the import walls limit by deselecting one or more wall or shelving types.

c) Click **Use Selected Layers**.

Step 7 Enter the floor map dimensions in the **Width**, **Length**, and **Height** fields.

Step 8 Click **Add**.

By default, the map is displayed with a grid. To turn the grid off or on, use the **Show Grid** toggle button at the bottom-left side of the map.

Note After you import a floor plan, make sure that you enable the overlay visibility. (From the floor, click **View Options** and enable the overlay toggles in **Overlay Objects**). By default, overlays are not displayed after you import a map.

Add a floor with a non-CAD map file

You can use non-CAD files (JPG, GIF, PNG, or PDF file types) to create a floor map. However, when using a non-CAD file, the 3D floor elements, such as walls and shelvings, cannot be imported, and you must add them manually later. For more information, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, hover your cursor over the ellipsis ••• next to the building and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Step 4 In the **Global Unit System** area, select **Feet** or **Meters**.

When the floor is added, all the floors across all the sites sync to display all measurements in your chosen unit system. To update the global unit system, see 2D map view options, on page 289.

Step 5 From the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 6 Drag and drop the non-CAD file (JPG, GIF, PNG, or PDF file type) onto the **Floor Image** area.

Note Ensure to provide the precise dimensions of floors that are in the PDF format, because the image width and height ratio cannot be extracted from them.

Step 7 Click **Add**.

The floor map is created.

Note After you import a floor plan, make sure that you enable overlay visibility. (From the floor, click **View Options** and in **Overlay Objects**, enable overlay visibility by clicking the overlay object's corresponding toggle button.) By default, overlays do not display after you import a map.

Step 8 To add walls as a 3D floor element:

a) From the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Walls**.

b) From the left pane of the map, click the wall type that you want to add.

If the wall type is not in the list, click **Add Wall Type** to create a new wall type.

c) Use the drawing tool to create a wall on the map:

- Click where you want to begin the wall. Then move your cursor to the next point and click again. Continue this process until you have created the wall in the shape you want.
- To finalize the wall, double click where you want the wall to end. To cancel the drawing, right-click the map.
- To change the type of an existing wall, right-click the shape and choose **Change Type**.
- To move an existing wall, drag and drop the shape to the new location.
- To remove an existing wall, right-click the shape and choose **Delete**.

Figure 7: Adding a wall with the drawing tool



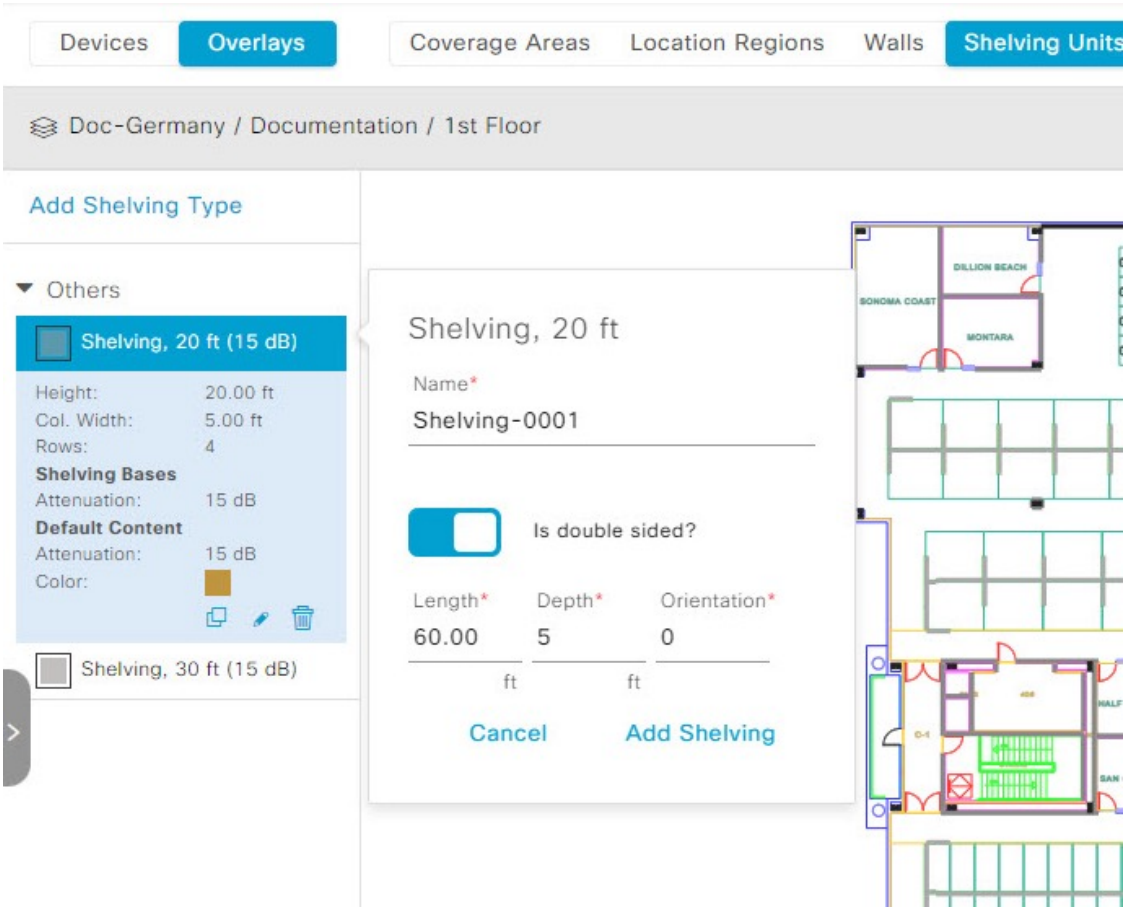
Step 9 To add shelving units as a 3D floor element:

a) In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Shelving Units**.

b) In the left pane of the map, click the shelving type that you want to add.

- In the **Shelving** dialog box, you can edit the name, dimensions, and orientation of the shelving type. Orientation refers to the angle of the shelving, for example, 0 means that the shelving is vertical and parallel to the y axis.
- If a shelving type is not in the list, click **Add Shelving Type** to create a new shelving type.

Figure 8: Choosing a shelving type to add



c) In the **Shelving** dialog box, click **Add Shelving** to add the shelving to the floor map.
d) Drag and drop the shelving to move it to a location on the floor map.
e) Right-click the shelving and choose one of these actions:

- **Edit**: Edit the name, dimensions, and orientation of the shelving.
- **Clone**: Create a copy of the shelving.
- **Array**: Create an array of shelving by specifying the number of shelves and the distance between them.
- **Remove**: Remove the shelving from the floor map.

Step 10 When you're done, click **Save** in the map toolbar.

Work with 2D maps

2D maps are primarily used to configure elements on a floor map and view heatmaps.

Using 2D maps, you can add floor map elements and overlays. While viewing a 2D map, you can manipulate the display of the various elements and overlays. You can also filter device data and identify wireless interferers.

Catalyst Center calculates the strength and quality of wireless signals. These RF predictions are commonly known as heatmaps, because they show the relative intensity of the RF signals on the 2D wireless coverages area map.

Prerequisite

For optimal computation and display of 2D wireless heatmaps, we recommend using a system with a Graphics Processing Unit (GPU) installed and enabled.

If your system does not have a GPU, or the GPU is disabled in your browser, be sure to toggle on the **Disable 3D-Computed Heatmap** option. (For information, see 2D map view options.) Otherwise, you may experience reduced performance, including high CPU usage. With this option enabled, you can continue using the 2D view, even without a GPU.

By default, the 3D-computed heatmap engine is used when viewing 2D maps in Catalyst Center 2.3.7.x. Enabling the **Disable 3D-Computed Heatmap** option switches to server-side heatmaps, as in earlier Catalyst Center releases.

2D floor map devices and overlay objects

In 2D maps, you can configure devices and overlay objects on your floor maps.

Devices

- **APs**: An access point (AP) serves as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In 2D maps, an AP represents an actual, installed device. For a list of APs that Catalyst Center supports, see the *Cisco Catalyst Center Compatibility Matrix*.
- **Planned APs**: Planned APs are representations of APs that haven't been installed yet. By placing planned APs on a map, you can envision your wireless network RF coverage and make changes before you actually install the APs.
- **Sensors**: A sensor is a dedicated Cisco Aironet 1800S Active Sensor that gets bootstrapped using Cisco PnP. After it obtains the Assurance server reachability details, it communicates directly with the Assurance server. For more details, including information about sensor tests, see the *Cisco Catalyst Assurance User Guide*.

Overlay objects

- **Coverage Areas**: By default, any area defined as part of a floor map is considered as a wireless coverage area. However, if you have a building that is nonrectangular or you want to mark a nonrectangular or polygon-shaped area on a floor, you can use the **Coverage Areas** drawing tool to create a coverage area.
- **Openings**: An opening, also called an atrium, is an open-air or skylight-covered area within a building. An opening can extend through multiple floors and can affect wireless signal coverage areas.
- **Location Regions**: Location regions are used by location services (Cisco CMX or Cisco Spaces). Location regions define areas that are included in or excluded while positioning clients. Inclusion areas are included in the calculations and exclusion areas aren't included. When you create a floor, by default, the whole region on the floor is defined as the inclusion region. You can manually edit the default inclusion region

and set exclusion regions on the floor. For example, you can exclude areas such as openings or atriums, and large racks within a building, where positioning of real clients isn't possible.

- **Walls**: Walls define any exterior or interior vertical structures in a building, such as windows, cubicles, and doors. Because they can be made of different materials and have different densities, they can significantly impact RF signal attenuation and heatmap calculation. For example, the more walls you include in a floor map, the longer it can take to compute a heatmap. Although, even if you have a high number of walls on your floormap, you can adjust the number used to compute the heatmap For information, see 2D map view options, on page 289 and 3D map view options, on page 302.
- **Shelving Units**: Shelving units are obstacles that can significantly impact RF signal attenuation and heatmap calculation. A high-ceiling warehouse is an example of a location with shelving units.
- **Markers**: A marker identifies a location on a map. When you create a marker, you can name it and position it to help you identify it later.
- **GPS Markers**: When integrated with Catalyst Center, location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), use GPS markers to calculate the approximate geographical location of clients.
- **Align Points**: Align points are markers that are used to position multiple floors that have different physical shapes. In 3D maps, floors are aligned at the top-left corner of the map (point 0,0). If you manage each floor independently, the misalignment isn't a problem. However, to use some of the features of 3D maps, the floors need to be aligned as they are in reality. To compensate for this misalignment, you can insert one or more align points on two or more floors, so that the floors align properly one on top of the other in a 3D map.

Work with APs on a floor map

Catalyst Center computes heatmaps for the entire map that show the relative intensity of the Radio Frequency (RF) signals in the coverage area. For 2D wireless maps, the heatmap is only an approximation of the actual RF signal intensity because it does not consider the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Follow these guidelines while placing APs on the floor map:

- Place APs along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. APs placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Therefore, location is difficult to determine. Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.
- For optimal heatmap visibility on floor maps, configure the AP height to approximately 10 feet (3 meters) or lower.

Export APs from Cisco Prime Infrastructure and import into Catalyst Center

Catalyst Center allows you to import, assign, and position a collection of APs to the floor map. If you have an existing collection of APs on Cisco Prime Infrastructure, you can import it into Catalyst Center, saving time and effort spent in importing, assigning, and positioning APs to the floor map.

This procedure describes how to export an existing collection of APs from Cisco Prime Infrastructure and to import it into Catalyst Center.

Before you begin

- To do this task, you must be a **Super Admin** or **Network Admin**.
- Make sure that you have APs in your inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- The area, building, and floor must be present in the site hierarchy.

Procedure

Step 1 Export the AP positions from Cisco Prime Infrastructure as a CSV file to your workstation.

Step 2 From the main menu, choose **Design** > **Network Hierarchy**.

Step 3 From the left hierarchy tree, hover your cursor over the ellipsis ••• next to the site and choose **Import Access Points**.

Alternatively, from the map toolbar, you can click **Import** and choose **Import Access Points**.

Step 4 In the **Import Access Points** dialog box, drag and drop the AP file, or click **Choose a file** to select the file from your workstation.

Note

- To manually create the **AP Positions** CSV file with the Prime template, export the Prime template to your workstation by clicking **Download Prime Template**. The Prime template does not support nested files.
- To manually create the **AP Positions** CSV file with the Catalyst Center template, export the Catalyst Center template to your workstation by clicking **Download Cisco Catalyst Center Template**. The Catalyst Center template supports nested files.

Wait for the CSV file to download. The CSV file contains information about the AP positions of various sites in the network.

Step 5 Click **Import**.

The **Import Summary** window displays.

- The **Information** tab shows the list of successfully imported APs.
- Click the **Warning** tab to see the list of warnings.
- Click the **Error** tab to see the list of errors.

Step 6 In the top-right corner of the **Import Summary** window, click **Done** to return to the **Network Hierarchy** window.

Add APs to a map

This procedure describes how to add APs to a floor map. You can add a maximum of 200 APs to a floor.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover them using the Discovery feature. See Discovery overview, on page 55.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 From the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 In the left pane of the map, click **Add Access Points**.

Step 5 In the **Add Access Points** slide-in pane, do one of these tasks in the table:

Task	Action
To add a single AP	Locate the AP that you want to add, and scroll to the right and click **Add**
To add multiple APs	Check the check boxes next to the APs you want to add, and click **Add Selected**.
To add all APs	Click **All APs**, and click **Add Selected**.
To add autolocate capable APs	Click **Auto Locate Capable APs**, and click **Add Selected**.

Note You can search for APs using the search option available. Use the **Filter** field to search for APs using the AP name, MAC address, model, or Cisco Wireless Controller. The search is case-insensitive. The search results appear in a table. Click **Add** to add one or more of these APs to the floor area.

In edit mode, newly added APs are displayed in the **Unpositioned** category in the map left pane. For more information, see Position an AP on a map, on page 265.

Step 6 After adding the APs to a floor, close the **Add Access Points** slide-in pane.

What to do next

When you add an AP to a map, the wireless map automatically stores this data even after the AP is deleted from the inventory:

- AP name
- AP MAC address
- Current site of the AP
- Current position of the AP on the map

Note If you delete the corresponding site from the network hierarchy, the stored AP data is also removed.

When you delete the wireless controller with all its managed APs from the inventory, Catalyst Center displays a planned AP icon for the corresponding APs on the map. For more information, see About the AP icon and planned AP icon, on page 292.

If the same AP is rediscovered in the inventory later, Catalyst Center automatically places it back on the map at the same site and position even if a different wireless controller manages it.

To remove the AP data from the map when the AP is deleted from the inventory, do one of these tasks:

- Before deleting the wireless controller from the inventory, assign the corresponding APs to the **Global** site. For more information, see Assign an unprovisioned device to a site, on page 156.
- After deleting the wireless controller from the inventory, remove the corresponding planned APs from the map. For more information, see Remove APs from a map, on page 275.

Add planned APs to a map

This procedure shows you how to use the AP Model Catalog feature to add a planned AP to a floor and configure its model, antenna type, azimuth, and elevation orientation. Using the planned AP that you just created and placed, you can add more planned APs with the same properties.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 In the left pane of the map, in the **Planned AP Models** area, click the AP model of the planned AP that you want to add.

Note If the AP model isn't listed, click **Add Model** and choose the AP model to add to the list.

Step 5 On the floor map, click the location where you want to place the planned AP.

A planned AP of the selected model is added to the floor map, and the **Edit Planned AP** slide-in pane is displayed with an AP name added to it by default.

Step 6 In the **Edit Planned AP** slide-in pane, click the gear icon that is located next to the **AP Name** field.

The **Name pattern** dialog box is displayed.

Step 7 When you add the first AP to the floor, make sure that you enter a valid name pattern, for example, SJC-BLD21-FL2-AP####, and then click **Set name pattern**.

Note The planned APs must be unique within Catalyst Center. So, make sure that the name pattern identifies the floor.

The #### in the name pattern is replaced by numbers in the **AP Name**, for example, SJC-BLD21-FL2-AP0001, SJC-BLD21-FL2-AP0002, and so on.

Step 8 From the **Antenna** drop-down list, choose the appropriate antenna type, including dual antennas, for the AP.

Note The antenna image reflects the selected antenna.

Step 9 Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation in degrees.

Step 10 (Optional) Configure any of the other settings, as needed. For information about these settings, see Edit an AP, on page 269.

Step 11 Do these tasks, as needed:

- To add another planned AP with the same properties as that of the planned AP that you just added, on the floor map, click a location where you want to position the new AP.

  A new AP icon displays on the map with all of the properties inherited and the AP name appended, for example, BLD1-AP0002-TX.

- To add more planned APs with the same properties and appended AP name, click the floor map.
- To stop adding planned APs to the floor map, press **Esc** or right-click the floor map.
- To reposition the planned APs, drag and drop them to the appropriate location in the floor map.
- To delete a planned AP, right-click the AP icon and click **Remove**.
- To edit a planned AP, right-click the AP icon and click **Edit**.
- To autoplace a planned AP, see Autoplace planned APs on a map, on page 261.

Step 12 In the map toolbar, click **Save**.

Autoplace planned APs on a map

Autoplacing planned APs on a floor map allows you to see how many planned APs can be placed within the dimensions of the map. Using the planned AP model, maximum distance you'd like between the planned APs, and coverage area dimensions, the system calculates the maximum number of planned APs placements and adds them to the floor map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 In the left pane of the map, click **Autoplace Planned APs**.

Step 5 In the **Autoplace Planned APs** dialog box, choose the AP model, enter the maximum distance you'd like between the planned APs, and enter a valid name pattern.

The #### in the name pattern is replaced by numbers in the planned AP name, for example, AP-0001, AP-0002, and so on.

Step 6 Click **Create**.

The system calculates the maximum number of planned APs placements and adds them to the floor map. The system automatically selects all the newly placed planned APs, and the **Edit APs** slide-in pane, where you can collectively edit all the new planned APs, displays.

Step 7 From the **Antenna** drop-down list, choose the antenna type.

Step 8 (Optional) To collectively update the planned APs, edit the available fields.

Step 9 Click **Apply** to apply the update to all the autoplaced planned APs.

Step 10 (Optional) Do these tasks, as needed:

- To edit a planned AP, either click the planned AP icon or right-click the planned AP icon and choose **Edit**.
- To stop editing a planned AP, press **Esc**, right-click the floor map, or close the **Edit Planned AP** slide-in pane.
- To reposition the planned APs, drag and drop them to the appropriate location in the floor map.
- To remove a planned AP, right-click the planned AP icon and choose **Remove**.

Step 11 When you're ready, click **Save** to save the changes to the map.

Auto locate APs on a map

The Auto Locate Access Points feature allows you to automatically position and locate your APs on the map. Using this feature, you can seamlessly and accurately position the APs on the map without any manual intervention and determine the precise location of the APs through a detailed map. Automatic and accurate positioning of APs helps in reducing the deployment time and cost in a new site addition or site expansion

scenarios and facilitates the remote management activities for APs. For more information on using the feature, see Guidelines and limitations for AP Auto Locate, on page 263.

Before you begin

Generate the AP measurement data. For more information, see Generate AP-to-AP measurement data, on page 264.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit/Locate**.

Step 4 If you do not have any APs placed on the floor map, follow the below steps to automatically position the APs:

a) Add Auto Locate-capable APs to the floor map. See Add APs to a map, on page 258.

b) In the left pane of the map, click **Auto Locate Access Points**.

The list of Auto Locate-capable APs is displayed in the left pane. Based on AP measurement data, APs are ranked automatically for anchor selection.

c) Position the anchor APs on the map.

From the left pane of the map, select an AP and drag and drop to the required location on the map. Position the remaining anchor APs similarly. You must select at least four anchor APs before you proceed to place the rest of the APs on the floor.

d) Click **Run Auto Locate** to automatically place the remaining APs on the map.

The APs are automatically positioned on the map and a pop-up window displays the AP Auto Locate summary.

e) In the **AP Auto Locate Summary** pop-up window, click **View Results**.

A detailed floor map with the placed APs is displayed. You can filter the results by anchor APs and the newly positioned APs.

f) Click **Save** to save the changes to the map.

Step 5 If you have APs already placed on the floor map, follow the below steps to locate the APs and verify their position:

a) In the left pane of the map, click **Auto Locate Access Points**.

b) Select the anchor APs on the map. You must select at least four anchor APs to proceed with Auto Locate.

c) Click **Run Auto Locate** in the AP floor map window.

A pop-up window displays the AP Auto Locate summary such as the number of anchor APs, properly positioned APs, and moved or swapped APs.

d) In the **AP Auto Locate Summary** pop-up window, click **View Results**.

The map displays the position of all the APs on the floor map with details such as anchor APs, properly positioned APs, and APs that have been moved or swapped. Choose the options in the left pane to filter the results. If there are any moved or swapped APs, the positions are corrected automatically.

e) Click **Save** to save the changes to the map.

f) Click **Run Auto Locate** again to verify that all APs are positioned properly.

Guidelines and limitations for AP Auto Locate

Guidelines and limitations while using the AP Auto Locate feature, include:

- In the current release, the Auto Locate feature is in beta state and requires feature enablement. Users are notified of the availability of the feature on the Catalyst Center home page and are redirected to the feature enabling window. After the feature is enabled, you can use the Auto Locate feature from the **Network Hierarchy** window. For more information on feature availability and activation, contact your Cisco sales representative.
- The feature is supported on all Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.12.x or later and on APs with Fine Timing Measurement (FTM), Wi-Fi 6E, and Wi-Fi 7 capabilities.

  For information about supported APs, refer to *Feature Matrix for Cisco Wireless Access Points*.

Note

- The AP ranging process may take up to 15 minutes on wireless controllers running Cisco IOS XE Release 17.12.x.
- AP ranging data cannot be collected for isolated APs that cannot receive the FTM signal.
- Currently, the feature is not supported on GPS-capable APs.

- The Auto Locate feature is supported for a maximum of 50 APs on a floor.
- The feature is not supported for multifloor APs. You can run Auto Locate for APs on one floor at a time.
- APs that are outside of the floor boundary are not considered for generating the AP measurement data.
- APs that do not have sufficient neighboring APs cannot be used for Auto Locate.
- AP to AP granular ranging is not supported.
- Provisioning and ranging is supported on APs that use shared site tags (tags shared across multiple floors).
- APs with default tags are not supported for generating measurement data.
- Not all anchor AP tags are exported when Catalyst Center is integrated with location services such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX). Interoperability between Catalyst Center and Cisco Spaces or CMX is not supported for the AP Auto Locate feature.
- Export and import of map archives with anchor tagging is not supported. You must manually tag the anchor APs after importing the map archive.
- The AP ranging process for generating AP measurement data may cause network disruptions for the connected clients. It is recommended to perform this process during off-peak hours.
- AP Auto Locate performance depends on the APs on the floor, their locations, the floor area, and the ranging data.

- AP measurement data is stored in Catalyst Center for 30 days only, after which it is deleted. You must retrigger the ranging process to generate the AP measurement data.
- It is recommended not to trigger the wireless controller reprovisioning during AP ranging process.

Generate AP-to-AP measurement data

Use this procedure to generate the AP measurement data for all the eligible APs on a floor. This data is used to automatically place or locate APs on the floor map.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover them using the Discovery feature. See Discovery overview, on page 55.

For guidelines and limitations on the AP ranging process, see Guidelines and limitations for AP Auto Locate, on page 263.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit/Locate**.

Step 4 In the left pane of the map, click **Auto Locate Access Points**.

Step 5 Review the anchoring best practices and click **Close**.

Step 6 Click **Generate AP to AP Measurement**.

The **Generate AP to AP Measurement** window displays all the APs on the floor that are eligible for measurement.

Step 7 Select the APs for measurement.

You have an option to choose all the eligible APs on the floor or select the required APs individually.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.



Note We recommend that you schedule the measurement process to run later, during off-peak hours, as it could cause network disruptions for connected clients.

Step 9 On the **Tasks** window, monitor the task deployment.

Assign actual APs to planned APs

After you install the actual APs in your wireless network, you can assign them to the planned APs on your map. This procedure describes how to assign planned APs to actual APs.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 In the left pane of the map, click **Assign Planned APs**.

Step 5 On the floor map, click a planned AP.

Step 6 In the **Assign Planned APs** slide-in pane, check the check box next to the AP that you want to assign.

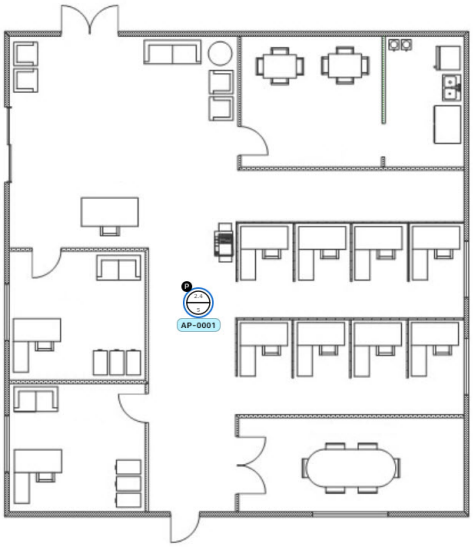
Step 7 Click **Assign**.

Step 8 In the map toolbar, click **Save**.

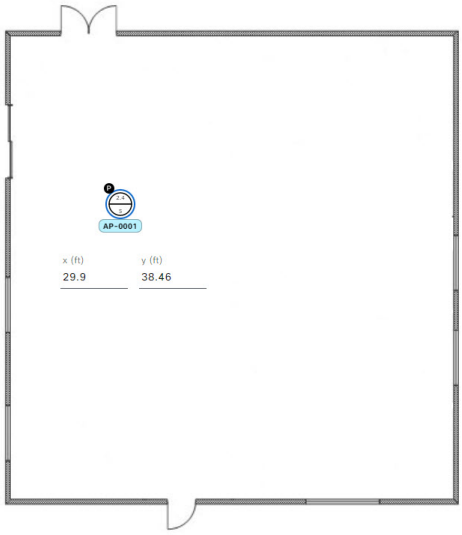
Position an AP on a map

After adding an AP to a floor, you must position it on the map using one of these methods:

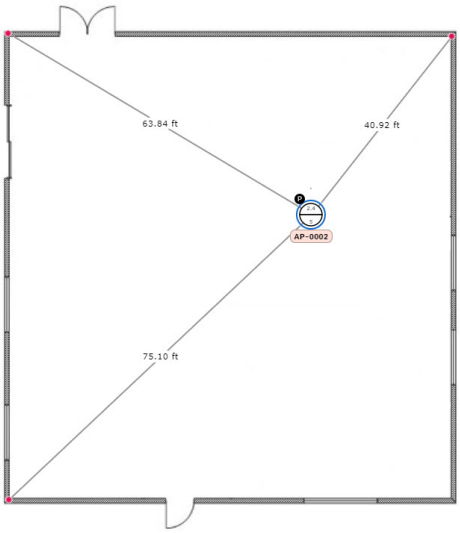
- Manually position it on the map. Use this method if you can approximate the location of the AP using reference points in the building that you can correlate to the detail on the floor map.



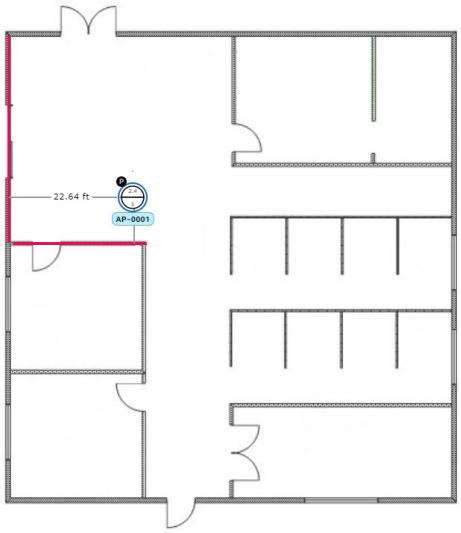
- Define its **x** and **y** coordinates. Use this method if you have the exact coordinates of the AP and you want its position on the map to be as accurate as possible.



- Triangulate it using 3 points. Use this method if you have large open space with only a few points from which to measure the distance to the AP. For example, you might measure from the AP to each corner of the room.



- Intersect it based on its distance from two walls. Use this method if the AP is located in a space where you have two walls that intersect, even if they aren't perpendicular to one another.



For all but the first method (manual positioning), you must have your measurements on hand, and make sure the unit of measure is specified correctly in the **Global Map Properties** settings. For information, see 2D map view options, on page 289.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

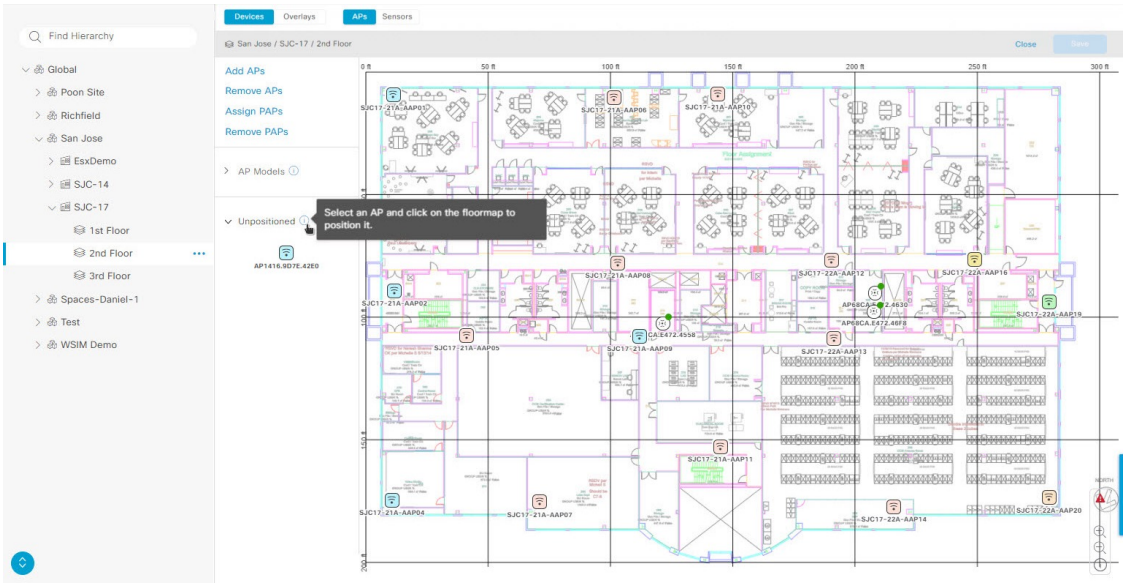
Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 From the left pane of the map, in the **Unpositioned** area, click an AP.

Figure 9: Unpositioned APs



Step 5 To position the AP, use one of these methods:

- Click the location on the floor map where you want to position the AP.
- Define its **x** and **y** coordinates in the **Edit AP** slide-in pane.
- Triangulate its location:

  a. In the **Edit AP** slide-in pane, click **3 points**.

  b. Click on floor map to draw the first point.

  c. In the dialog box, set the distance from the AP to the first point and click **Set Distance**.

  d. Define the second and third points similarly, and click **Save**.

- Define two walls on the floor map and position the APs between the defined walls:

  a. In the **Edit AP** slide-in pane, click **2 walls**.

  b. To define the first wall, click the floor map to start drawing the line. Click again to finish drawing the line.

  A dialog box is displayed to set the distance from the AP to the first wall.

  c. Enter the distance in meters, and click **Set Distance**.

  d. Define the second wall similarly, making sure that the distance to the AP from the first and second walls create an intersecting point.

  e. Click **Save**.

  The AP is placed based on the defined distance between the walls.

Step 6 In the map toolbar, click **Save**.

Note If Cisco Connected Mobile Experiences (CMX) is synchronized with Catalyst Center, you can view the location of clients on the heatmap. See Create Cisco CMX settings, on page 442.

Reposition an AP on a map

After you position APs on a map, you can reposition them. This procedure shows you how to reposition an AP on a map.

Note You can perform this task in a 2D or 3D map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 For 2D:

a) In the map toolbar, click **2D** > **Add/Edit**.

b) On the map, drag and drop the AP to the new position.

Step 4 For 3D:

a) In the map toolbar, click **3D** > **Edit/Clone**.

b) On the map, right-click the AP and choose **Move**.

c) On the map, drag and drop the AP to the new position.

Step 5 In the map toolbar, click **Save**.

Edit an AP

Use this procedure to edit the configuration of a single AP or planned AP.

To change the configuration of multiple APs at the same time, see Edit multiple APs, on page 272.

Note You can do this task in a 2D or 3D map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 Depending on the wireless map type, click the AP that you want to edit.

If you are working with a...	Then...
2D wireless map	**a.** In the map toolbar, click **2D** > **Add/Edit**. **b.** On the map, right-click the AP and choose **Edit**.
3D wireless map	**a.** In the map toolbar, click **3D** > **Edit/Clone**. **b.** On the map, click the AP that you want to edit.

Step 4 In the slide-in pane, edit any of the available AP and planned AP settings.

- **AP Name** or **Planned AP Name**: Name of the AP.
- **MAC Address**: MAC address of the selected AP.
- **AP Model**: Model of the selected AP.



Note For APs in 3D maps, you can change the **AP Model** field to visualize its impact, but the changes aren't saved and don't persist across floors. Instead, you can update this AP field from the **Inventory** window.

- **x (ft)**: X-axis coordinate of the AP.
- **y (ft)**: Y-axis coordinate of the AP.
- **AP Height (ft)**: Height of the AP.
- **Antenna**: Antenna type for this AP.



Note For external APs, you must choose an antenna. If you don't choose an antenna, the AP will not be present on the map.

- **Channel**: Channel to be used by the AP. Only channels that are supported by the AP model are displayed.



Note For APs in 3D maps, you can change the **Channel** field to visualize its impact, but the changes aren't saved and don't persist across floors. Instead, you can update this AP field from the **Inventory** window.

- **Tx Power (dBm)**: Transmit power for the channel. Only power levels that are supported by the channel are displayed.

Note For APs in 3D maps, you can change the **Tx Power (dBm)** field to visualize its impact, but the changes aren't saved and don't persist across floors. Instead, you can update this AP field from the **Inventory** window.

- **Azimuth**: Angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is from 0 to 360. In Catalyst Center, pointing right is 0 degrees or 360 degrees; pointing down is 90 degrees.

  You can manually enter the value or use the blue arrow under the field to change the value.

  Note For omnidirectional antennas, the azimuth is not relevant if the elevation is 0.

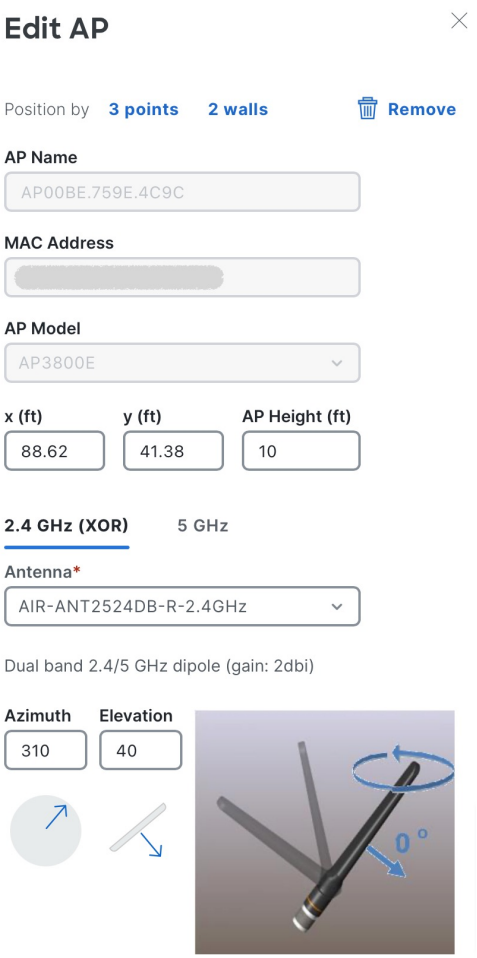
- **Elevation**: Measured in degrees.

  You can manually enter the value or use the blue arrow under the field to change the value.

  Note If this field is disabled, it is dimmed and displays the tilt value reported from the AP. This disablement means that the AP radio supports accelerometer hardware and that the accelerometer feature is enabled on the AP.

Note For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values mean pointing down.

Figure 10: Edit AP slide-in pane



Step 5 After making the edits, use this table to proceed.

If you are working with a...	Then...
2D wireless map	Close the slide-in pane.
3D wireless map	Click **Apply** to apply the changes.

Step 6 In the map toolbar, click **Save**.

Edit multiple APs

When you select only one AP or planned AP, you can change all editable attributes. However, when you select multiple APs or planned APs, only some attributes are editable, including:

- When the selected devices have the same value for an attribute, the value is displayed. Otherwise, the value is blank. In either case, if you change the value, the new value is applied to all the selected devices.

- When the selected APs have the same model number and radios (number of radios and operating band), the antennas are editable. Otherwise, they are not editable.
- You can change the model numbers of planned APs but not added APs. So, if you select an AP, the model number is not editable.
- Because bulk changes affect more devices, they do not take effect immediately. You must click **Apply** to apply your changes.

This procedure shows you how to update the editable attributes for multiple APs at the same time.

Note You can perform this task in a 2D or 3D map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 Do one of these tasks:

- For 2D, in the map toolbar, click **2D** > **Add/Edit**.
- For 3D, in the map toolbar, click **3D** > **Edit/Clone**.

Step 4 Select the APs, using one of these methods:

- Click the first device, then press and hold the **Shift** key while you click the rest of the devices.
- In the 2D map navigation controls toolbar, click the select by rectangle icon ( ). Then click an area of the map and drag the highlighted rectangle to select APs in a contiguous area. All the highlighted APs within the rectangle are selected.

To deselect APs, use one of these methods:

- To deselect a single AP, press and hold the **Shift** key while you click the AP.
- To deselect all APs except one, click the AP you want to remain selected. All others are deselected.
- To deselect all APs, press the **ESC** key or close the **Edit** pane.

Step 5 In the slide-in pane, configure the settings of the APs, as available:

- **AP Name** or **Planned AP Name**: Name of the AP.
- **MAC Address**: MAC address of the selected AP.
- **AP Model**: Model of the selected AP.

Note For APs in 3D maps, you can change the **AP Model** field to visualize its impact, but the changes aren't saved and don't persist across floors. Instead, you can update this AP field from the **Inventory** window.

- **x**: X-axis coordinate of the AP. You can manually enter the value.
- **y**: Y-axis coordinate of the AP. You can manually enter the value.
- **AP Height**: Height of the AP. You can manually enter the value.
- **Antenna**: Antenna type for this AP.

Note For external APs, you must select an antenna, or the AP will not be present in the map.

- **Channel**: Channel to be used by the AP. Only channels that are supported by the AP model display.

Note For APs in 3D maps, you can change the **Channel** field to visualize its impact, but the changes aren't saved and don't persist across floors. Instead, you can update this AP field from the **Inventory** window.

- **Tx Power (dBm)**: Transmit power for the channel. Only power levels that are supported by the channel are displayed.

Note For APs in 3D maps, you can change the **Tx Power (dBm)** field to visualize its impact, but the changes aren't saved and don't persist across floors. Instead, you can update this AP field from the **Inventory** window.

- **Azimuth**: Angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is from 0 through 360. In Catalyst Center, pointing right is 0 degrees or 360 degrees; pointing down is 90 degrees.

  You can manually enter the value or use the blue arrow under the field to change the value.

Note For omnidirectional antennas, the azimuth is not relevant if the elevation is 0.

- **Elevation**: In degrees. You can manually enter the value or use the blue arrow under the field to change the value.

Note For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values mean pointing down.

Step 6 In the slide-in pane, click **Apply** to apply the changes.

Step 7 In the map toolbar, click **Save**.

Remove APs from a map

This procedure shows you how to remove APs and planned APs (PAPs) from a map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

Step 4 To remove APs (including planned APs):

a) Click the AP. To select multiple APs, click the first AP and while pressing the **Shift** key, click the rest of the APs.

b) In the slide-in pane, click **Remove**.

Step 5 In the map toolbar, click **Save**.

Work with sensors on a floor map

These topics show you how to add sensors to floor maps and position, reposition, and delete them, if needed.

For more information about sensors, see 2D floor map devices and overlay objects, on page 255.

Add sensors to a map

This procedure shows you how to add sensors to a map.

Before you begin

Make sure you have the Cisco AP 1800S sensor in your inventory. The Cisco Aironet 1800s Active Sensor must be provisioned using Plug and Play for it to show up in the Inventory. See the "Provision the Wireless Cisco Aironet 1800s Active Sensor" topic in the *Cisco Catalyst Assurance User Guide*.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Sensors**.

Step 4 In the **Add Sensors** slide-in pane, check the check boxes of the sensors that you want to add. Alternatively, click **Add** next to the sensor row.

Note You can search for specific sensors using the **Filter** field. Search using the name, MAC address, or model of a sensor. The search is not case-sensitive. The results are displayed in the table. Click **Add** to add one or more of these sensors to the floor area.

Newly added sensors are displayed in the **Unpositioned** category in the left pane of the map in edit mode.

Step 5 In the map toolbar, click **Save**.

Position sensors on a map

Newly added sensors are displayed in the **Unpositioned** category in the left pane of the map in edit mode. This procedure shows you how to position a sensor after initially adding it.

Before you begin

Sensors must be added to the map before they can be positioned. For information, see Add sensors to a map, on page 275

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Sensors**.

Step 4 In the left pane of the map, click a sensor in the **Unpositioned** category to position the sensor.

Step 5 On the floor map, click the location where you want to position the sensor.

You can use the **x**, **y**, and **Height** fields in the **Sensor Details** slide-in pane to enter the exact x, y, and z coordinates for the sensor.

Step 6 In the map toolbar, click **Save**.

Reposition a sensor on a map

After you position sensors on a map, you can reposition them. This procedure shows you how to reposition a sensor on a map.

Note You can do this task in a 2D or 3D map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, do one of these tasks:

- Click **2D** > **Add/Edit**.
- Click **3D** > **Edit/Clone**.

Step 4 On the map, drag and drop the sensor to the new position.

Step 5 In the map toolbar, click **Save**.

Remove sensors from a map

This procedure shows you how to remove sensors from a floor map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit**.

Step 4 To remove sensors, do these tasks:

a) Click the sensor, or to select multiple sensors, click the first sensor and while pressing the **Shift** key, click the rest of the sensors.

b) In the **Edit** pane, click **Remove**.

Step 5 In the map toolbar, click **Save**.

Add, edit, and remove coverage areas

This procedure shows you how to mark a nonrectangular or polygon-shaped area as a coverage area on a floor map.

For more information about coverage areas, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Coverage Areas**.

Step 4 To add a coverage area, do these tasks:

a) In the **Coverage Area** dialog box, enter a name for the coverage area in the field.
b) Click **Add Coverage**.
c) Click on the map to create a point and initiate the drawing tool.
d) Continue creating points to define the coverage area shape.

Note The coverage area shape must have at least three points. Click and drag a point to redefine the coverage area shape.

e) Double-click to exit the drawing tool and finalize the coverage area shape.

Step 5 To edit a coverage area, do these tasks:

a) In the map toolbar, click **Add/Edit** > **Coverage Areas**.
b) To redefine the shape of a coverage area, click and drag a point.
c) To edit a coverage area name, right-click the coverage area and select **Edit**.

Step 6 To delete a coverage area, do these tasks:

a) In the map toolbar, click **Add/Edit** > **Coverage Areas**.
b) Right-click the coverage area and select **Remove**.

Step 7 In the map toolbar, click **Save**.

Add, edit, copy, and remove openings

Creating an opening is similar to creating an open space or atrium on a floor. On multifloor buildings, typically the opening extends vertically through multiple floors. This procedure shows you how to add, edit, and remove openings on a floor map. It also shows you how to copy openings to other floors.

For more information about openings, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Openings**.

Step 4 To add an opening:

a) From the left pane of the map, click **Opening**.
b) Click on the map to create a point and initiate the drawing tool.
c) Continue creating points to define the opening shape.

Note The opening shape must have at least three points. Click and drag a point to redefine the opening shape.

d) Double-click to exit the drawing tool and finalize the shape.

Step 5 To edit an opening:

a) In the map toolbar, click **Add/Edit** > **Openings**.
b) To redefine the shape of an opening, click and drag a point.
c) To move an opening, click inside the shaded area. Then, drag and drop the opening where you want to place it.

Step 6 To copy an opening from one floor to another:

a) In the map toolbar, click **Add/Edit** > **Openings**.
b) Right-click the opening and select **Copy to other floors**.
c) In the dialog box, check the check boxes next to the relevant floors.
d) Click **Copy**.
e) Click **Close**.

Step 7 To remove an opening:

a) In the map toolbar, click **Add/Edit** > **Openings**.
b) Right-click the opening and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove location regions

Location regions are areas on the map that are either included in or excluded from the heatmap calculation. These topics show you how to add, edit, and remove location regions.

Add, edit, and remove an inclusion region

This procedure shows you how to add, edit, and remove an inclusion region. Use these guidelines to define an inclusion region on a floor map:

- Inclusion regions can be any polygon-shaped area and must have at least three points.
- You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

For more information about inclusion regions, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.
Step 2 From the left hierarchy tree, select a floor.
Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Location Regions**.
Step 4 In the left pane of the map, click the **Inclusion** icon.
Step 5 To create an inclusion region, use the drawing tool:

a) Click the map to create a point where you want the inclusion region to begin.
b) Move the cursor to the next point and click again.

c) Continue creating points to define the inclusion region shape.
d) To finalize the shape, double-click the map.

Alternatively, from the left pane of the map, click the **Inclusion** icon.

e) To exit the drawing tool, double-click the map again.

Step 6 To edit the location of an inclusion region, drag and drop the shape to the new location.

Step 7 To remove an inclusion region, right-click the shape and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove an exclusion region

This procedure shows you how to add, edit, and remove an exclusion region. Use these guidelines to define exclusion regions on a floor map:

- Exclusion regions can be any polygon-shaped area and must have at least three points.
- Exclusion regions are defined within the borders of an inclusion region.
- You can define multiple exclusion regions on a floor map.

For more information about exclusion regions, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Location Regions**.

Step 4 From the left pane of the map, click the **Exclusion** icon.

Step 5 To create an exclusion region, use the drawing tool:

a) Click the map to create a point where you want the exclusion region to begin.
b) Move the cursor to the next point and click again.
c) Continue creating points to define the exclusion region shape.
d) To finalize the shape, double-click the map.

Alternatively, from the map left pane, click the **Exclusion** icon.

e) To exit the drawing tool, double-click the map again.

Step 6 To edit the location of an exclusion region, drag and drop the shape to the new location.

Step 7 To remove an exclusion region, right-click the shape and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove walls

This procedure shows you how to add, edit, move, and remove walls on a floor map.

For information about how walls impact RF signal attenuation and heatmap calculation, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Walls**.

Step 4 To add walls:

a) In the left pane of the map, click a wall type from the **Others** or **On this floor** category.

Note If a wall type isn't listed, click **Add Wall Type** to create a custom wall type.

b) Click the map to create a point where you want the wall to begin.

c) Move the cursor to the next point, where you want to end the wall or where you want to create a corner and click again.

d) Continue creating points to define the wall shape.

e) To end a wall, double-click the map.

Alternatively, from the left pane, click the wall type.

f) To exit the drawing tool, double-click the map again.

Step 5 To change a wall type, and depending on the wall type also configure its parameters:

a) Click the wall that you want to change.

The **Wall Type** dialog box opens.

b) From the **Wall Type** drop-down list, select the type of wall.

c) Configure any other parameters that are appropriate for the new wall type.

d) Click **Update**.

Step 6 To move a wall:

a) Hover your cursor over the wall that you want to move.

The wall turns black, which means it's selected.

b) Click the wall and drag and drop it to the new location.

Step 7 To remove a wall, right-click the wall and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, copy, edit, and remove shelving units

This procedure shows you how to add, copy, edit, and remove shelving units on a floor map.

For information about shelving units, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Shelving Units**.

Step 4 To add shelving units:

a) In the left pane of the map, click the shelving type you want to add.

b) In the shelving dialog box, configure the name, dimensions, orientation, and whether the unit is double-sided, or leave the default values. Orientation means the angle of the shelving unit. A shelving unit with an orientation of zero means that the shelving unit is vertical and parallel to the y-axis.

If a shelving type is not in the list, click **Add Shelving Type** to create a shelving type.

c) Click **Add Shelving**.

The shelving unit appears on the map.

d) Drag and drop the shelving unit to its location on the map.

Step 5 To create a copy or an array of a shelving unit:

- To create a copy, right-click the shelving unit and select **Clone**.
- To create an array, right-click the shelving unit and select **Array**. Then specify the number of units and the distance between them.

Step 6 To edit the name, dimensions, orientation, and whether it is two-sided, right-click the shelving unit and select **Edit**.

Step 7 To remove a shelving unit, right-click the shelving unit and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove markers

This procedure shows you how to add, edit, and remove markers.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Markers**.

Step 4 In the left pane of the map, click the **Markers** icon.

Step 5 In the **Place Markers** dialog box, enter the name for the marker, and click **Add**.

Step 6 To place the marker, click the map where you want to place the marker.

Step 7 To move a marker, hover your cursor over the marker until it turns blue. Then drag and drop it in the new location.

Step 8 To edit a marker, right-click the marker and select **Edit**.

Step 9 To remove a marker, right-click the marker and select **Remove**.

Step 10 In the map toolbar, click **Save**.

Add, edit, and remove GPS markers

This procedure shows you how to add, edit, and remove GPS markers. For more information about GPS markers, see 2D floor map devices and overlay objects, on page 255.

Note The GPS marker is an attribute of the building. You can apply it to all the floors of the building.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **GPS Markers**.

Step 4 To add a GPS marker:

a) In the left pane of the map, click the **GPS Markers** icon.

b) On the map, click the location where you want to place the GPS marker.

GPS markers must be positioned inside the outer-perimeter walls, typically at the building corners.

c) In the **Place Markers** dialog box, enter the name, latitude, longitude, and the x and y coordinates in the appropriate fields.

The latitude and longitude coordinates of the GPS marker located in the northwest corner of a floor must match the building coordinates.

d) Click **Add**.

To include GPS markers in calculations, you must add at least three GPS markers.

Step 5 To edit a GPS marker, right-click the GPS marker and select **Edit**.

Step 6 To move a GPS marker, hover the cursor over the marker until it turns orange. Then drag and drop it in the new location.

Step 7 To remove a GPS marker, right-click the GPS marker and select **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, edit, and remove align points

This procedure shows you how to add, edit, and remove align points. For more information about align points, see 2D floor map devices and overlay objects, on page 255.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Align Points**.

Step 4 To add an align point:

a) In the left pane of the map, click the **Align Points** icon.

b) On the map, click the location where you want to place the align point.

Step 5 To edit the name of an align point:

a) Right-click the align point and select **Edit**.

b) Change the name and click **Update**.

Step 6 To change the location of an align point:

- Hover your cursor over the align point until it turns blue. Then drag and drop it in the new location.
- Right-click the align point and select **Edit**. Update its **x** and **y** coordinates and click **Update**.

Step 7 To remove an align point, right-click the align point and select **Remove**.

Step 8 In the map toolbar, click **Save**.

View a 2D wireless heatmap

Use this procedure to view the 2D wireless heatmap and information about your wireless network.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D**.

The wireless 2D map opens.

Step 4 Display specific details about devices using this list based on the device type.

- **APs**: The AP icon indicates the number of radios, their frequency and health, overall health score of the device, and the AP name and mode. For more information about interpreting the AP icon, see About the AP icon and planned AP icon, on page 292.

  To display device details, hover your cursor over an AP icon. Information, such as the AP Rx neighbors, clients, interferers, health score, and license noncompliance, is displayed.

  For more details about an AP, in the dialog box, click the **Device 360** link.

Note For **Device 360**, the *Assurance - Base* package is required.

- **Mesh APs**: To display device details, hover your cursor over a mesh AP icon. Information, such as mesh, backhaul, and access data, is displayed.
- **Clients**: To display client information, including a link to its associated AP, hover your cursor over or click a client. For more details about a client, in the dialog box, click the **Client 360** link.
- **Sensors**: To view the status and test results of a sensor, click a sensor icon.
- **Switches and Switch Stacks**: To display the member switches of a switch stack, click the arrow next to the switch stack icon. To display the connections between a switch and its associated APs, hover your cursor over the switch or switch stack icon. The map displays a line showing the connections from the switch and its associated APs. You can also identify switch and AP associations by color. APs connected to one specific switch have labels that match the color code on the switch icon.

  Using Cisco Discovery Protocol (CDP), Catalyst Center can detect and display unmanaged switches that are connected to managed APs. An unmanaged switch is depicted as a typical switch icon with a "U" for unmanaged ( ).

  To display device details, click a switch or switch stack icon. A slide-in pane opens and displays the device details and options for the heatmap display. Under **Select Heatmap**, you can click any of these radio buttons:

  - **All visible switches**: Computes and displays the heatmap for all the switches in the visible map area.
  - **This switch**: Computes and displays the heatmap for the selected switch only.
  - **Rest of visible switches**: Computes and displays the heatmap for all of the visible switches, except for the selected switch.
  - **None**: Does not include any switch in the heatmap computation and heatmap display.

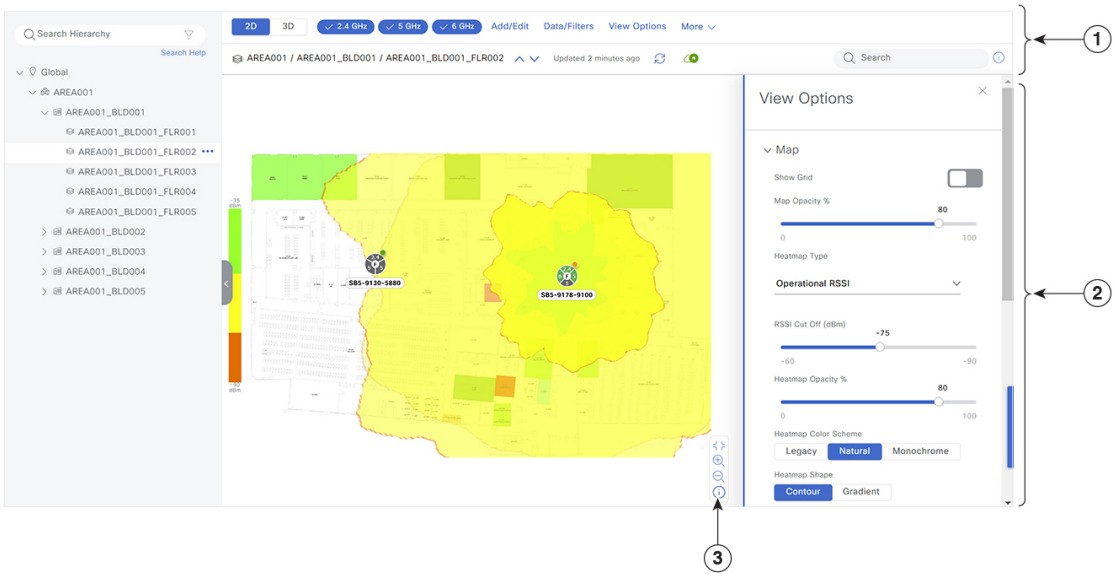
Step 5 To display information about a link, click the link.

Depending on the type of link, information such as link health and other statistics are displayed.

For a mesh link, you can perform a link test between two mesh APs.

Step 6 Use the tools and options displayed in the 2D wireless heatmap to gain insights about your wireless network.

Figure 11: 2D Wireless Map Showing Tools and Options



Callout	Description
1	**Map Toolbar**: Above the map, use the toolbar options to control what's displayed on the heatmap. For details, see 2D map toolbar, on page 286.
2	**View Options Slide-In Pane**: In the slide-in pane, use the view options to customize the heatmap display. For information, see 2D map view options, on page 289.
3	**Navigation Controls**: From the bottom-right corner of the map, use the map navigation controls to manage the heatmap display. For details, see 2D map navigation controls, on page 292.

2D map toolbar

To access the 2D map, from the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, select a floor, and in the map toolbar, click **2D**.

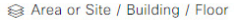
The map toolbar consists of two bars and is located above the map. Use the map toolbar to control heatmap displays and do actions, such as adding and editing devices and overlay objects.

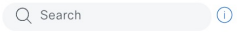
Item	Description
2D 3D	Click **2D** to view the wireless map in 2D, or click **3D** to view it in 3D.
2.4 GHz 5 GHz 6 GHz	Click a Wi-Fi band button to choose the corresponding Wi-Fi band filter. You can choose multiple Wi-Fi bands.

Item	Description

Add/Edit	Click this button to add, edit, and remove devices and overlay objects.
	• **Devices**
	  • **Access points**: For details, see Work with APs on a floor map, on page 256.
	  • **Sensors**: For details, see Add sensors to a map, on page 275.
	• **Overlay Objects**
	  • **Coverage areas**: For details, see Add, edit, and remove coverage areas, on page 277.
	  • **Openings**: For details, see Add, edit, copy, and remove openings, on page 278.
	  • **Location regions**: For details, see Add, edit, and remove location regions, on page 279.
	  • **Walls**: For details, see Add, edit, and remove walls, on page 280.
	  • **Shelving Units**: For details, see Add, copy, edit, and remove shelving units, on page 281.
	  • **Markers**: For details, see Add, edit, and remove markers, on page 282.
	  • **GPS markers**: For details, see Add, edit, and remove GPS markers, on page 283.
	  • **Align points**: For details, see Add, edit, and remove align points, on page 283.

Data/Filters	Click **Data/Filters** to open the **Data/Filters** slide-in pane that displays a device type list. Choose a device type to view and filter the device data that displays in the wireless map. For details, see Filter device data on a floor, on page 295.
View Options	Click **View Options** to open the **View Options** slide-in pane, which contains the options for controlling the display of the map, devices, and overlay objects. For details, see 2D map view options, on page 289.

Item	Description
More	Hover your cursor over **More**, and from the drop-down list, choose an available option. • **Recompute**: Recompute the heatmap. • **Export**: Export the floor map to a PDF or CSV file format. • **Edit Floor**: Change the floor details, such as its name. • **Set Scale**: Change the map scale by providing a known measurement on the map: 1. Click the map to specify the starting point of the measurement. 2. Click the map again to specify the ending point of the measurement. 3. In the **New line length (ft)** field, enter the length of the measurement. 4. Click **OK**. The floor map dimensions are recalculated based on the new measurement. • **Measure Distance**: Measure a distance on the floor map. Click the map to specify a starting point. Click the map again to specify an ending point. The distance of the measurement is displayed. • **CMX/Cisco Spaces Sync History**: Display a log that shows when Cisco Connected Mobile Experiences (CMX) and Cisco Spaces synchronized data. The log entries include the request received time, start and end times, status, and failure message (if the operation failed). • **Floor Import History**: Display the floor import history logs of importing map archive files. The logs detail the successfully and unsuccessfully imported APs, planned APs, and overlay objects.
	**Full Hierarchy Path**: Displays the full navigational path of the floor, including its associated building and area or site. Click the down arrow to navigate to a different floor.
	**Refresh**: Click this icon to update the device and map data. To the left of the icon is the timestamp for the last refresh.
	**Cisco Spaces Connector**: Click this icon to display information, such as the IP address, status, and version, about the Cisco Spaces Connector.
	**Map Notification**: Hover your cursor over this icon to display map information, such as the number of unpositioned APs or planned APs and filters applied to the map. To remove the filters, click **Click to clear**.
	**Error**: Displays an error notification (for example, AP license noncompliance). Click the corresponding hyperlink to view the details.

Item	Description
	**Search**: Use the **Search** field to find specific floor map elements such as APs, sensors, clients, and so on. The results of your search are listed in a slide-in pane below the **Search** field. When you hover your cursor over an element in the list, an indicator points to the element on the map. If the element is outside the field of view, the indicator is displayed as a broken red line. Reorient the map to see the element.

2D map view options

To access the 2D map, from the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, select a floor, and in the map toolbar, click **2D** > **View Options**.

The **View Options** slide-in pane opens. Expand the categories to view the settings:

- **Map**: Contains various floor map and heatmap settings:

Item	Description
Show Grid	Click this toggle button to enable or disable a grid on the floor map. The grid provides the dimensions of the floor map.
Map Opacity %	Use this slider to customize the opacity or transparency of the floor map.
Heatmap Type	The heatmap provides a graphical representation of Radio Frequency (RF) wireless data where the values taken by a variable are represented in maps as colors. RSSI heatmaps are computed based on a floor's RSSI prediction model, antenna type, and its orientation. 2D heatmaps use fixed transmit powers: 18 dB for 2.4-GHz; 15 dB for 5-GHz; and 5 dB for 6-GHz. 3D heatmaps use real-time transmit power of operational APs and 11 dB for planned APs. Use the drop-down list to choose the heatmap type: • **Operational RSSI**: Coverage heatmap, which identifies the wireless signal strength of operational APs. • **Planned RSSI**: Hypothetical heatmap that shows the coverage that planned APs would have on a floor. • **Operational + Planned (3D-only)**: (Visible only if the legacy heatmap generator is enabled.) In the 2D map, only operational APs are used to compute the heatmap. To use operational and planned APs in the heatmap computation, you can either enable the 3D-computed heatmap generator or navigate to the 3D map. For information, see the **Disable 3D-Computed Heatmap** field in this topic. • **Operational + Planned**: (Visible only if the 3D-computed heatmap generator is enabled.) Coverage heatmap created using both operational and planned APs. • **Client Density**: Density of associated clients. • **IDS**: Heatmap that shows the monitor mode AP coverage provided to the wireless clients on a floor map.

Item	Description
RSSI Cut off (dBm)	Use this slider to set the threshold for the RSSI value to appear on the heatmap. RSSI values that do not meet the threshold are faded.
Heatmap Opacity %	Use this slider to customize the opacity or transparency of the heatmap.
Heatmap Color Scheme	Customize the color scheme of the power level for the heatmap. The options are **Legacy**, **Natural**, and **Monochrome**. Note that **Monochrome** only supports the **Contour** option for the **Heatmap Shape**.
Heatmap Shape	Customize the color progression of the power level on the heatmap. The options are **Contour** and **Gradient**.

- **Access Points**: Click this toggle button to enable or disable the AP icons on the floor map.

  Expand this category to configure the type of label to display with each AP. From the **Display Label** drop-down list, choose up to four label types.

  To display other details about APs, see View a 2D wireless heatmap, on page 284.

- **Planned Access Points**: Click this toggle button to enable or disable the appearance of planned AP icons on the floor map.

  Expand this category to configure the type of label to display with each planned AP. From the **Display Label** drop-down list, choose up to two label types.

- **Switches**: Click this toggle button to enable or disable the appearance of switch or switch stack icons on the floor map. Using Cisco Discovery Protocol (CDP), Catalyst Center can detect and display unmanaged switches that are connected to managed APs. An unmanaged switch is depicted as a typical switch icon with a "U" for unmanaged.

  Expand this category to display labels with the switch name, MAC address, or AP count. (For unmanaged switches, only the switch name and AP count are available.) From the **Display Label** drop-down list, choose a label type.

  To display other details about switches, see View a 2D wireless heatmap, on page 284.

- **Sensors**: Click this toggle button to enable or disable the appearance of sensor icons on the floor map.

  Expand this category to display labels with the sensor name, MAC address, or AP count. From the **Display Label** drop-down list, choose a label type.

  To display other details about sensors, see View a 2D wireless heatmap, on page 284.

- **Mesh**: Click this toggle button to enable or disable the appearance of mesh APs on the floor map.

  Expand this category to configure options that control how the mesh AP-to-root AP link relationships are displayed:

  - **Link Label**: To disable link labels, click the **None** radio button. To display labels for link signal-to-noise ratios, click the **Link SNR** radio button. To display labels for packet error rates, click the **Packet Error Rate** radio button. The link label setting is reflected on the map immediately.
  - **Link Color**: To disable link color, click the **None** radio button. To display link signal-to-noise ratios in color, click the **Link SNR** radio button. To display packet error rates in color, click the **Packet Error Rate** radio button.

    The link color settings are reflected on the map immediately. See the table for color definitions.

Link color	Link signal noise ratio (SNR)	Packet error rate (PER)
●	Represents an SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
●	Represents an SNR between 20 dB and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
●	Represents an SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

- **Mesh Parent-Child Hierarchical View**: Choose which mesh APs to display. From this drop-down list, choose **Select Only Root APs**, **Select up to 1st hops**, **Select up to 2nd hops**, **Select up to 3rd hops**, **Select up to 4th hops**, or **Select All**.

- **Overlay Objects**: Expand this category and click any of the overlay objects to enable or disable the overlay objects on the floor map.
- **Clients**: Click this toggle button to enable or disable the appearance of client icons on the floor map.

  Expand this category to display labels with the client name, MAC address, or AP count. From the **Display Label** drop-down list, choose a label type.

  To enable or disable clients in close proximity to be grouped together, click the **Show Client Clusters** toggle button.
- **Interferers**: Click this toggle button to enable or disable the appearance of client icons on the floor map.

  Expand this category to enable or disable the appearance of a zone of impact from interferers. Click the **Show Zone of Impact** toggle button.
- **Map Properties**: Expand this category to configure these settings on the map:
  - **Auto Refresh**: From this drop-down list, choose a time interval for the map display to be refreshed.
  - **Heatmap Walls Limit**: (Available only with the 3D-computed heatmap generator.) Enter the number of walls to be used in the heatmap computation. The more walls included, the longer it takes to compute the heatmap. The default and recommended limit is 3000.
  - **Mesh SNR Colors** and **Mesh PER Colors**: (Available only when mesh devices are present.) Enter the threshold ranges and their corresponding colors.
- **Global Map Properties**: Expand this category to configure these settings for all wireless maps:
  - **Units of Measure**: From the drop-down list, choose either **Feet** (imperial system) or **Meters** (metric system).
  - **Disable 3D-Computed Heatmap**: Click this toggle button to disable the default 3D-computed heatmap generator and enable the legacy heatmap generator. Be aware that computation and rendering using the legacy heatmap generator is not as fast as the 3D-computed heatmap, and you can't configure a limit on the number of walls to be included to compute the heatmap. (The **Heatmap Walls Limit** field is removed from the display.) The maximum number of walls using the legacy heatmap generator is 300, after optimization. If your floor map contains more, Catalyst Center alerts you and preserves the 300 most relevant walls (based on the length of the wall multiplied by its attenuation).

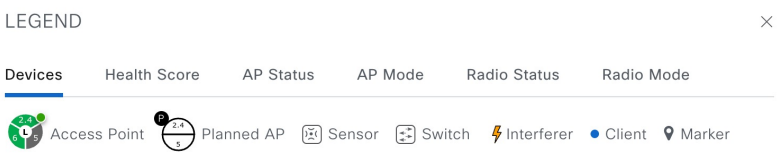
The 3D-computed heatmap generator offers several advantages over the legacy heatmap generator. It uses the specialized graphics processing unit (GPU), which allows it to generate the heatmaps substantially faster than the legacy heatmap generator. In addition, you can set a limit to the number of walls that are included in a heatmap computation, which also helps to enhance processing speed.

2D map navigation controls

To access the 2D map, from the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, select a floor, and in the map toolbar, click **2D**.

The 2D map navigation controls are located at the bottom-right of the map. For details about the map, see View a 2D wireless heatmap, on page 284.

Use the map navigation controls for these functions:

Map Navigation Controls	Description
	**Select by rectangle**: Displays only in editing mode. Use this icon to select multiple APs in a contiguous area on the map. First click this icon, then click an area on the map, and drag the highlighted rectangle. All the highlighted APs within the rectangle are selected.
	**Alert**: This icon displays when you choose to remove a banner notification without first resolving the error by clicking **Do not show this alert anymore**. When the error is resolved, the system doesn't display this alert icon.
	**Default Map View**: Click to reset the map view to the default.
	**Zoom In / Zoom Out**: Click the zoom in and out icons to enlarge and reduce the size of the map. Alternatively, you can use your mouse wheel to zoom in and out.
	Map Legend: Click this icon to view the map legend, which describes the map icons such as the device type, average health score, and AP status. For more information about the AP icon and planned AP icon, see About the AP icon and planned AP icon, on page 292. 

About the AP icon and planned AP icon

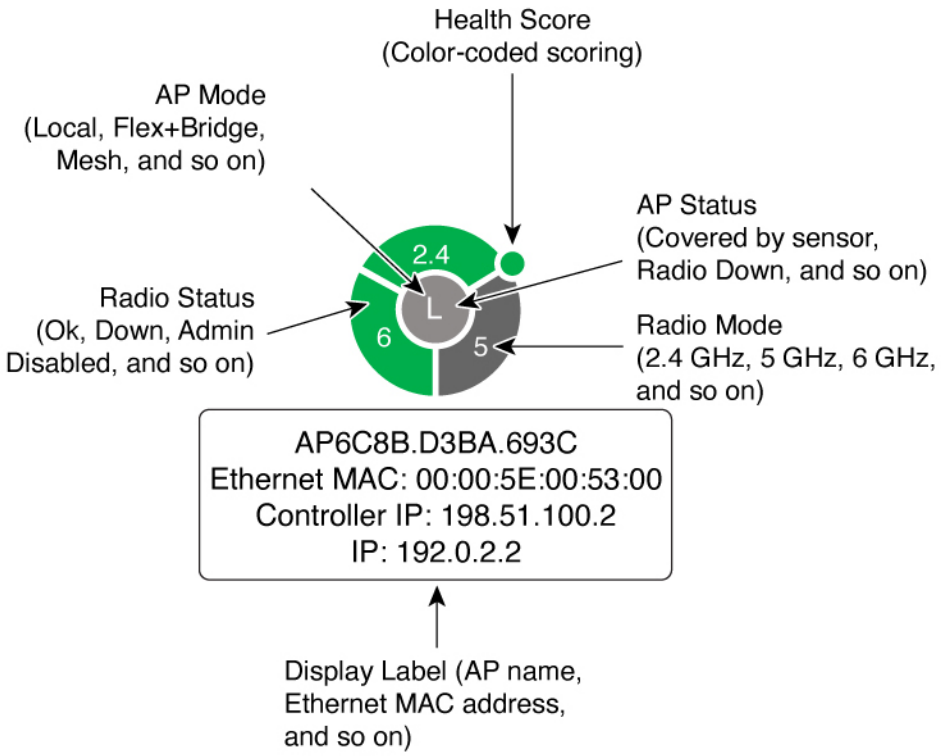
AP icon

AP icons provide information about the configuration and health of the APs in your network. The circular AP icon is divided into radio bands that are color-coded to show the radio status. Its center circle displays a letter for the AP mode. The background color of or "X" over its center circle shows the AP status. The color-coded small circle in the upper-right corner of the AP icon displays the health score.

For details on these functions, see the map legend on a 2D floor map:

- letters used for the AP mode,
- radio mode, and
- color coding of the radio status, AP status, and health score

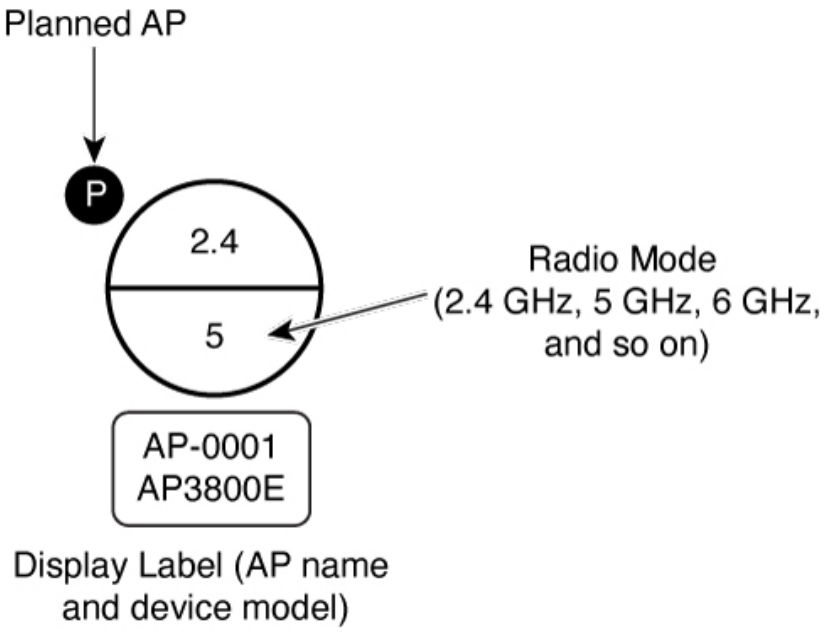
This diagram shows all the elements of an AP icon:



Planned AP icon

Planned AP icons provide information about the configuration of the planned APs in your network. The circular planned AP icon is divided into radio bands and displays a "P" in its upper-left corner. For more information about the radio mode, see the map legend in a 2D floor map.

This diagram shows all the elements of a planned AP icon:



View an unmanaged switch connected to managed APs

Catalyst Center can detect the unmanaged switches in your network and the managed APs to which they are connected. The unmanaged switches and their connections to APs can be displayed in a 2D floor map. This capability is helpful if you have switches that you don't want to manage using Catalyst Center, but you still want to view them in relation to your managed APs.

Note This feature isn’t supported on Cisco AireOS Wireless Controllers.

Before you begin

- Install and configure Catalyst Center Platform. For information, see the *Cisco Catalyst Center Platform User Guide*.
- Enable Cisco Catalyst Assurance. For information, see the *Cisco Catalyst Assurance User Guide*
- Add the wireless controller to the Catalyst Center Inventory, assign it to a site, and ensure that the device controllability configurations are pushed to the wireless controller. For information, see "Device Controllability" in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D**.

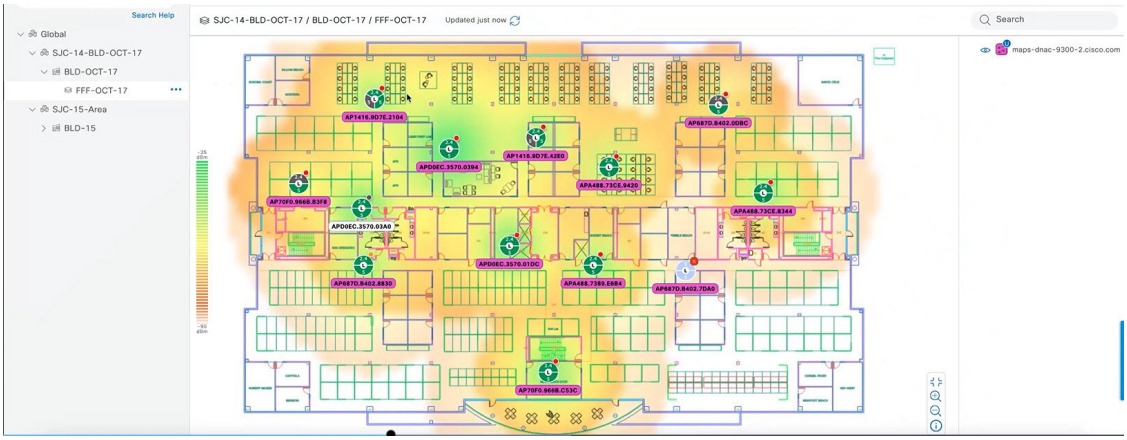
The wireless 2D map opens and displays the APs that have been added.

Step 4 Add APs to the floor map. For information, see Add APs to a map, on page 258.

Note If an AP is in Local, Bridge, or FlexConnect mode, connect it to the unmanaged switch and join it to a wireless controller.

After Catalyst Center refreshes the display, any unmanaged switches are listed in the right pane.

An unmanaged switch is depicted as a typical switch icon with a "U" for unmanaged ( ).



Step 5 (Optional) Hover your cursor over an unmanaged switch to display links between the switch and the APs to which it's connected.

Step 6 (Optional) Click the unmanaged switch to display additional details about the switch in a slide-in pane. All information that is available for managed switches is also available for unmanaged switches, except for the MAC address and its reachability status.

For more information about the elements, tools, and options available on 2D maps, see View a 2D wireless heatmap, on page 284.

Filter device data on a floor

For 2D wireless maps, you can apply various filters to network devices such as APs, sensors, and so on. Based on the filter criteria, the search results display in a table. Filtering device data is helpful in locating specific devices on floors with many devices.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D**.

Step 4 In the map toolbar, click **Data/Filters**.

Step 5 In the **Data/Filters** slide-in pane, click the device type that you want to apply a filter to.

Step 6 Define the filter rules by using the drop-down lists to choose the parameters.

Step 7 To add more filter rules, click the + icon near the top of the slide-in pane.

Step 8 To customize the columns displayed in the table:

a. In the top-right corner of the table, click the three vertical dots.

b. To display a column, check the check box next to the column name.

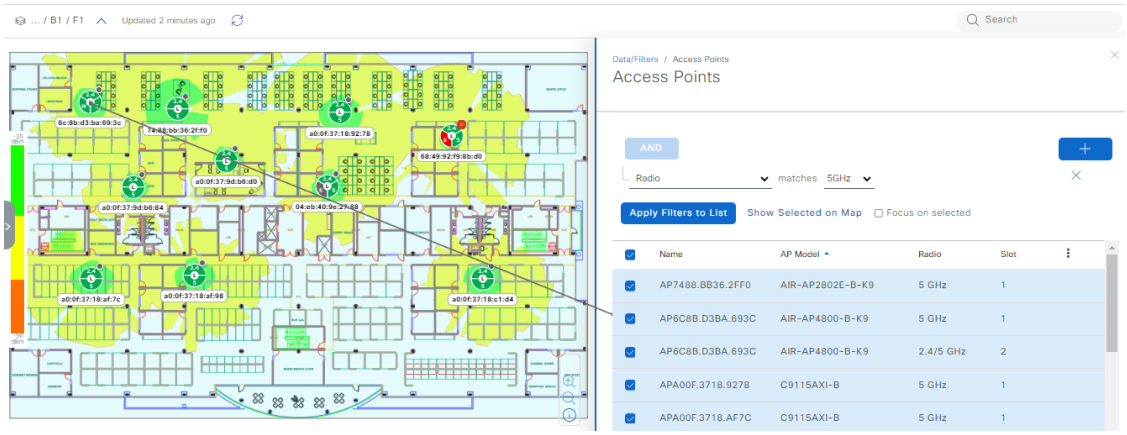
c. To hide a column, uncheck the check box next to the column name.

d. Click **Apply**.

Step 9 When you're done, you can do any of these tasks:

- To display the results of your filter in the table, click **Apply Filters to List**.
- To display the results of your filter in the map, click **Show Selected on Map**.
- To locate the position of a device on the map, hover your cursor over the device in the table. A line is displayed from the device to its position on the map.

Figure 12: Locating a device from the filter results



Step 10 To remove applied filters, in the lower map toolbar, hover your cursor over the notifications icon and click **Click to clear**.

Step 11 To return to the **Data/Filters** slide-in pane, click **Data/Filters** from the navigation path in the top-left corner.

Step 12 To close the slide-in pane and save the filter, click **x**.

Identify wireless interferers on the floor map

This feature is a 2D map feature.

Catalyst Center can detect interference and disable the interference source for a specific band on a floor map. Any interference in the 2.4-GHz band disrupts the network traffic of the 802.11 wireless network.

Catalyst Center can identify the position, area of impact, and intensity of the interferer.

This procedure shows how to identify network interferers on a floor map.

Before you begin

Ensure that either Cisco Connected Mobile Experiences (CMX) or Cisco Spaces is integrated with Catalyst Center. For information, see About Cisco Spaces integration, on page 444.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **2D**.

Step 4 In the **Network Hierarchy** window, click **View Options**.

Step 5 In the **View Options** window, scroll down and click the **Interferers** toggle button to enable interferers to be displayed on the floor map.

Step 6 Expand the **Interferers** category and click the **Show Zone of Impact** toggle button to enable the zone of impact of interferers to appear on the floor map.

Note By default, **Zone of Impact** is disabled.

Step 7 On the floor map, hover your cursor over the interferer icon and click the impacted channel to view the interferer device details.

Work with 3D maps

3D maps are primarily used to plan and analyze a wireless network on a floor. As such, there are minimal configuration and edit functions that you can perform in 3D maps.

With 3D wireless maps, you can view a 3D representation of your wireless network. A near real-time predictive model dynamically updates the 3D map to show changes in RF coverage.

Prerequisite

The system you use to compute and display 3D wireless heatmaps must have a Graphical Processing Unit (GPU) installed and enabled on it. For example, if you're using a Windows virtual machine (VM), you need to make sure that it has a GPU.

3D maps features and functionality

Here are some of the unique features and functionality that 3D wireless maps offers:

- Navigate through your wireless network in a 3D environment with a first person view or third person view.

- Gain insights into the areas in your wireless network where service-level agreements (SLAs) are not being met.
- Run an optimizer tool to compute the best AP layout to meet your SLAs.
- View the RF coverage for different elevations and use the **Scanner** tool to view the RF coverage for specific elevations.
- Crop the Key Performance Indicator (KPI) heatmap with the clipping tools.
- Predict the x, y, z coordinates of a specific point on the floor plan with the pin tool to better plan for placement of APs or sensors.
- Visualize floor plan elements, such as walls, in 3D to see how they affect RF coverage and attenuation.
- Simulate your wireless network in various configurations to see how the wireless coverage on a floor is affected. You can save these simulations and open them later to make more changes.
- Modify KPIs, telemetry, and 3D map element settings to customize your map display.

Configure floor map elements and overlays in 3D maps

In 3D maps, you are limited to these configurations and edit functions:

- Clone an AP, on page 298
- Edit an AP, on page 269
- Edit multiple APs, on page 272
- Reposition an AP on a map, on page 269
- Reposition a sensor on a map, on page 276

To configure other floor map elements or overlays, you need to use the 2D map. For details, see 2D floor map devices and overlay objects, on page 255.

Clone an AP

You can duplicate an AP with its configuration by cloning it.

Before you begin

You must have actual APs to clone.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 In the map toolbar, click the **Simulation** toggle button to view the map in simulation mode.

Step 5 In the map toolbar, click **Edit/Clone**.

Step 6 On the map, click an AP.

Step 7 In the **AP Details** slide-in pane, click **Clone**.

A duplicate AP is created and displayed below the original AP. Its name is appended with **-1**. If you keep cloning the same AP, the name continues to be incrementally appended. For example, the first clone for **a-floor1-ap01** is named **a-floor1-ap01-1**, the second clone for the same AP is named **a-floor1-ap01-2**, and so on.

Step 8 On the map, right-click the cloned AP and choose **Move**.

Step 9 Drag and drop the AP to its new position.

Step 10 Click **Save**.

View a 3D wireless heatmap

Use this procedure to view a 3D wireless map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

The 3D wireless map opens.

Note A 3D heatmap is delimited by its coverage area, which is the full floor width and length, by default. To specify a polygon for the heatmap boundaries, click **2D** > **Add/Edit** > **Overlays** and, in the left pane of the map, click **Coverage Area**. You can add and edit the coverage area in the 2D map. However, these boundaries don't apply to the 2D map view because the full floor width and length are used for the 2D map view.

Step 4 To display specific details about devices, hover your cursor over the device icon. Information about the device is displayed in a dialog box.

Note If the *Assurance - Base* package is installed, a link to the **Device 360** window is also displayed in the dialog box.

Step 5 To view the heatmap for one or more APs, select and deselect the APs using one of these methods:

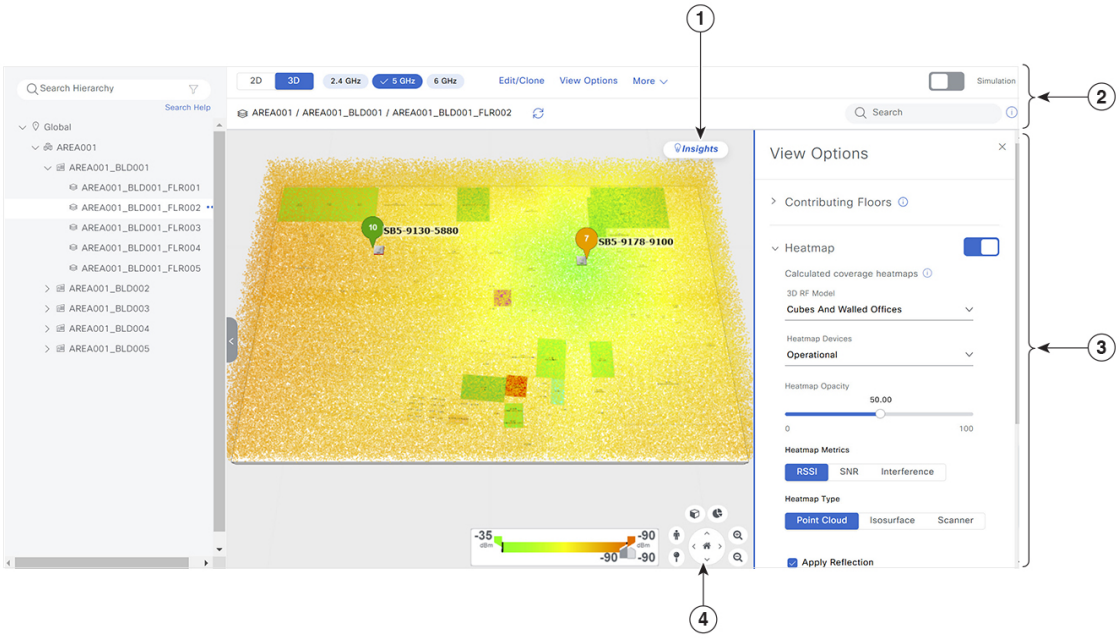
- To select a single AP, click the AP.
- To select multiple APs, press the **Shift** key while clicking each AP, and then release the **Shift** key.
- To deselect a single AP, click the AP.

Note If no APs are selected, the heatmap includes all APs.

- To deselect all APs, press the **ESC** key or double-click an area of the map that doesn't have any APs.

Step 6 Use the tools and options shown in the figure to gain insights about your wireless network.

Figure 13: 3D wireless map showing tools and options

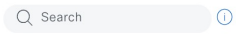


Callout	Description
1	**Insights Option**: In the top-right corner of the map, click **Insights** to view and understand potential issues in your wireless network. For details, see Gain insights from a 3D wireless map, on page 311.
2	**Map Toolbar**: Above the map, use the toolbar options to control what's displayed on the heatmap. For details, see 3D wireless map toolbar, on page 301.
3	**View Options Slide-In Pane**: In the slide-in pane, use the view options to control the heatmap display. You can manipulate elements, such as which floors are displayed, heatmap coverage and metrics, telemetry thresholds, devices and clients, overlay objects, and the depiction of a floor and sky. For details, see 3D map view options, on page 302.
4	**Navigation Controls**: In the bottom-right corner of the map, use the map navigation controls to view the heatmap from various perspectives. For details, see 3D map navigation controls, on page 304.

3D wireless map toolbar

To access the 3D map, from the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, select a floor, and in the map toolbar, click **3D**.

The map toolbar consists of two bars and is located above the map. Use the map toolbar to control heatmap displays and do actions, such as creating simulations of your wireless network.

Item	Description
	Click **3D** to view the wireless map in 3D, or click **2D** to view it in 2D.
	Click a Wi-Fi band button to choose the corresponding Wi-Fi band filter.
Edit/Clone	Click **Edit/Clone** to edit or clone existing or planned APs. For details, see Clone an AP, on page 298. **Note** Adding operational APs from the inventory is not available in the 3D map. To add operational APs, click **Add/Edit** in the 2D map toolbar.
View Options	Click **View Options** to open the **View Options** slide-in pane, which contains the options for controlling the display of the contributing floors, map, telemetry, devices, overlay objects, and floor geometry. For details, see 3D map view options, on page 302.
More	Hover your cursor over **More**, and click **Insights Configuration** to customize the conditions for insights. For details, see Gain insights from a 3D wireless map, on page 311.
Simulation	Click the **Simulation** toggle button to view the map in simulation mode. When the 3D wireless map enters simulation mode, the lower map toolbar displays the message: "You are in Simulation Mode". For details, see Create simulations for 3D wireless maps, on page 313. **Note** Simulation mode is available only in 3D maps, not in 2D maps.
	Full Hierarchy Path: Displays the full navigational path of the floor, including its associated building and site.
	**Refresh**: Click the refresh icon to update the device and map data.
	**Search**: Use the **Search** field to find specific floor map elements such as APs, sensors, clients, and so on. The results of your search are listed in a slide-in pane below the **Search** field. When you hover your cursor over an element in the list, an indicator points to the element on the map. If the element is outside the field of view, the indicator is displayed as a broken red line. Reorient the map to see the element.

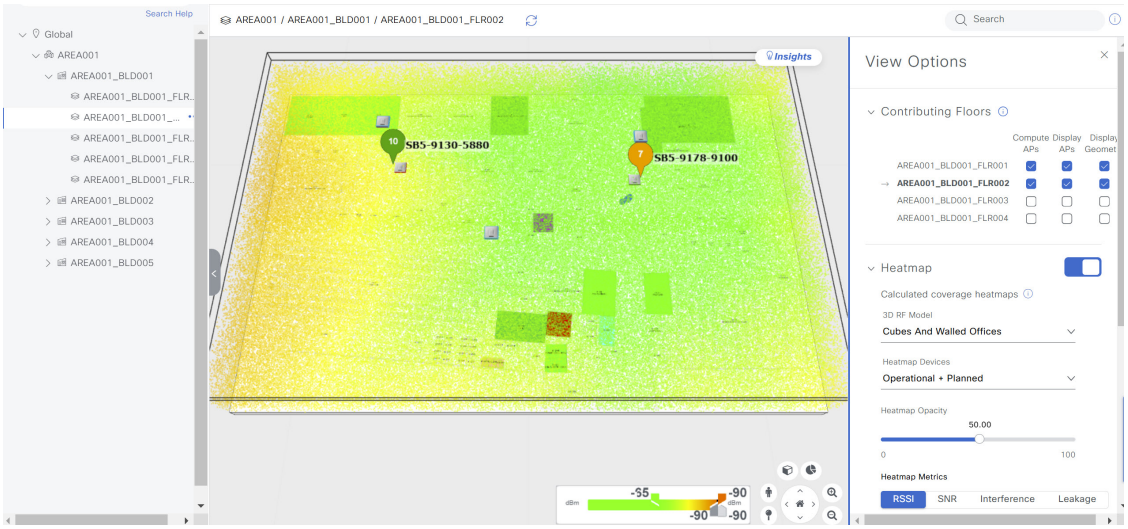
3D map view options

To access the 3D map, from the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, select a floor, and in the map toolbar, click **3D** > **View Options**.

The **View Options** slide-in pane opens. Expand the categories to view the settings:

- **Contributing Floors**: Expand this option to include more floors in the heatmap computation. When including a floor, you can choose to add its APs in the heatmap computation and display its APs and floor geometry. Click **Apply** to generate the heatmap with your settings.

Figure 14: 3D map of multiple floors



Item	Description
Compute APs	Check this check box to include the APs on a floor when computing the heatmap.
Display APs	Check this check box to display the APs on a floor in the heatmap.
Display Geometry	Check this check box to display the physical attributes of a floor in the heatmap.

- **Heatmap**: Click the **Heatmap** toggle button to display the heatmap, and expand this option to configure the settings using this table:

Item	Description
3D RF Model	Use this drop-down list to choose the RF model. The RF model determines how RF is calculated based on the floor geometry. Available models include drywall offices, cubes and walled offices, free space, outdoor open space, and indoor high ceiling. **Note** We recommend that you choose **Free Space** if you manually placed the walls or imported them from a CAD file or Ekahau project. If you didn't manually place the walls, use an RF model other than **Free Space**.

Item	Description
Heatmap Devices	Use this drop-down list to choose whether to display operational devices, operational and planned devices, or only planned devices on the heatmap.
Heatmap Opacity	Use this slider to customize the opacity or transparency of the heatmap.
Heatmap Metrics	Choose the type of metrics to display on the heatmap: • **RSSI**: Displays the Received Signal Strength Indicator (RSSI) values. • **SNR**: Displays the signal-to-noise ratio (SNR) values. • **Interference**: Displays the SNR that is caused by co-channel interference (CCI) or adjacent channel interference. • **Leakage**: Displays signal leakage between floors. For this option to be available, you must compute the heatmap with two or more contributing floors.
Heatmap Type	Choose the heatmap type: • **Point Cloud**: Provides a collection of data points in space. Each data point has x, y, and z coordinates. • **Isosurface**: Represents the RSSI with isolines or lines of a contiguous value. • **Scanner**: Displays the RSSI for a specific elevation.
Apply Reflection	Check this check box to show signal reflection, which can be caused when a signal bounces off materials such as glass, whiteboards, and plastic.

- **Telemetry**: Click the **Telemetry** toggle button to enable and disable telemetry. When telemetry is enabled, click a sensor or AP to view its telemetry:
  - The telemetry for a sensor displays the predicted and measured RSSI values between a sensor AP and other APs.
  - The telemetry for an AP displays the predicted and measured RSSI values between neighbor APs.

  Expand this option to use the **Telemetry Threshold** slider to set the threshold for telemetry sources to be displayed on the heatmap. Telemetry sources with predicted values that don't meet the threshold are faded.

- **Devices**: Expand this option to configure the settings using this table:

Item	Description
APs	Check this check box to display APs on the map.
Planned APs	Check this check box to display planned APs on the map.
Sensors	Check this check box to display sensors on the map.

Item	Description
Clients	Check this check box to display clients on the map. Additionally, you can do these tasks: • Display clients in their default blue color (**None**) or by their **RSSI**, **SNR**, or **Health Score**. For **RSSI**, **SNR**, and **Health Score**, clients are colored blue, yellow, or red, depending on their current condition. • Use the **Ball Size** slider to change the size of the ball that represents a client on the map.

- **Overlay Objects**: Expand this option to configure the settings using this table:

Item	Description
Geometry	Check this check box to display the floor geometry.
Height	Use this slider to set the height of walls on the heatmap.

- **Map**: Expand this option to configure the settings using this table:

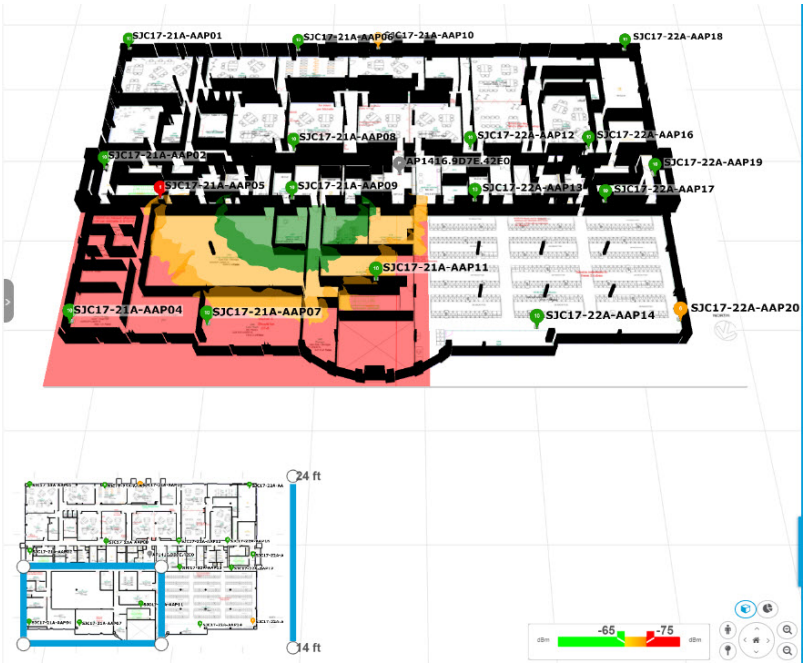
Item	Description
Sky	Check this check box to display the sky in the heatmap.
Floor	Check this check box to display the floor in the heatmap.

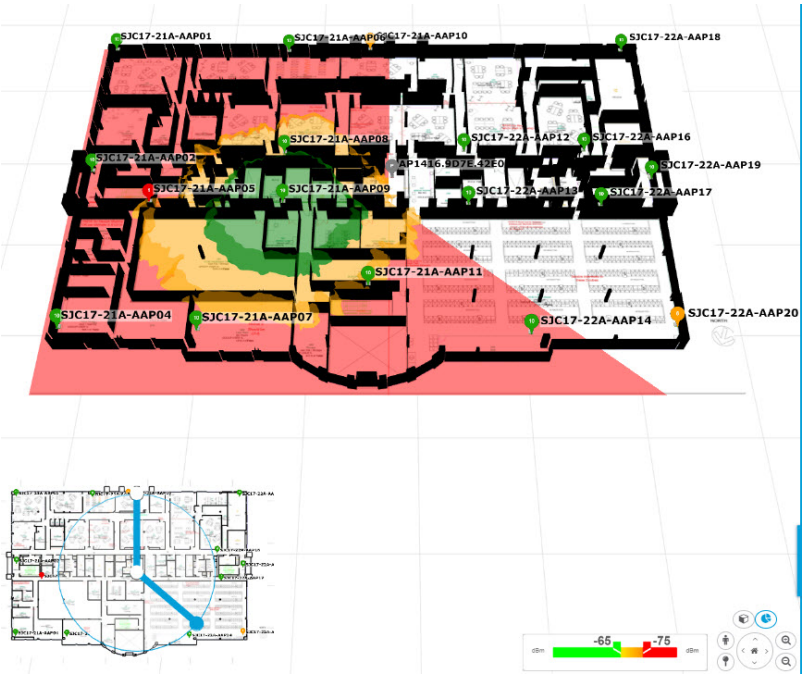
3D map navigation controls

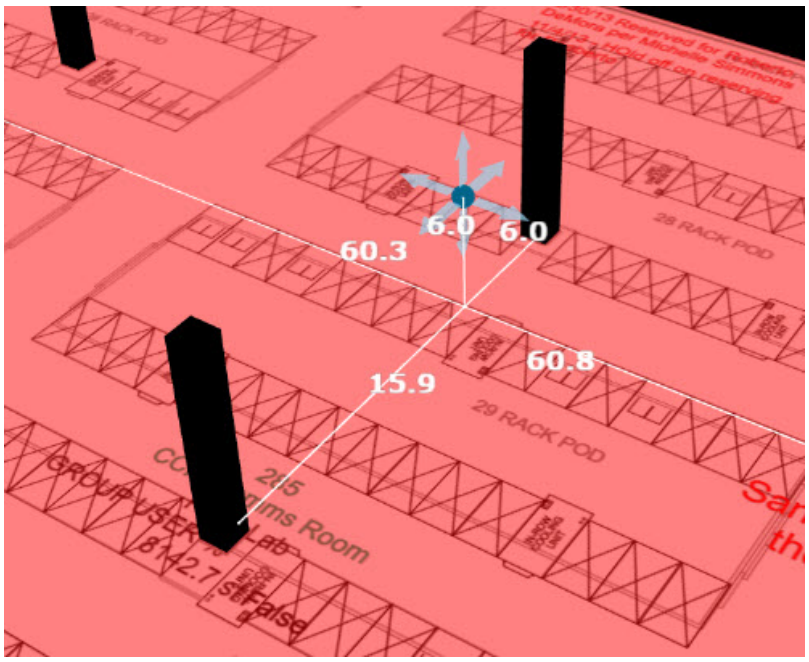
To access the 2D map, from the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, select a floor, and in the map toolbar, click **3D**.

The 3D map navigation controls are located at the bottom-right corner of the map. For details about the map, see View a 3D wireless heatmap, on page 299.

Use the map navigation controls at the bottom-right corner of the map to control the map view.

Map navigation control	Description
	**Use clip box**: Click this icon to crop the heatmap using a box shape. Use the clipper at the bottom-left corner of the map to specify the crop: • Click and drag one of the anchor points to change the size of the crop. • Click and drag one of the anchor points on the right vertical slider to specify the height range of the crop. ***Figure 15: Clip box*** 

Map navigation control	Description
	**Use clip planes**: Click this icon to crop the heatmap using a donut shape. Use the clipper at the bottom-left corner of the map to specify the crop: • Click and drag the anchor point in the center of the donut to reposition the donut. • Click and drag the two outer anchor points to change the shape of the crop. ***Figure 16: Clip planes in use*** 
	**First Person View**: Click this icon to switch between first-person view and third-person view. The blue sphere indicates your position on the map. As you move throughout the map, your field of view changes. You can use the mini map at the lower-left corner to get an idea of your field of view and orientation. **Note** If you have more than one floor selected for display, the **First Person View** automatically positions you on the current floor. For details, such as the controls for view, see Use first-person and third-person views for 3D wireless maps, on page 308.

Map navigation control	Description
	**Third Person View**: Click this icon to switch between first person view and third person view. You can also drag and drop the icon on the map where you want to be positioned. The blue sphere indicates your position on the map. As you move throughout the map, your field of view changes. You can use the mini map at the lower-left corner to get an idea of your field of view and orientation. For details, such as the controls for view, see Use first-person and third-person views for 3D wireless maps, on page 308.
	**Place a pin**: Click this icon to view a predicted measurement (x, y, and z coordinates) of a specific point on the floor map. By placing a pin, you can view the measurements of the distance from the pin to the end of the yard stick. As you zoom in or zoom out, the position of the measurements is adjusted to stay in your view. Drag and drop the pin to change its position. • **To move the pin horizontally**: Click the horizontal arrows and drag the pin left, right, forward, or backward. The selected arrows and yard stick are highlighted while active. • **To move the pin vertically**: Click the vertical arrows and drag the pin up or down. The selected arrows and yard stick are highlighted while active. For a video demonstration, click here. ***Figure 17: Adjusting a pin*** 
	**Zoom In**: Click this icon to enlarge the view. Alternatively, you can use your mouse wheel to zoom in.

Map navigation control	Description
	**Zoom Out**: Click this icon to reduce the size of the image and to increase your field of view. Alternatively, you can use the scroll wheel on your mouse to zoom out.
	**Map Rotation and Default Map View**: Click the directional arrows to change the camera angle. Click the Return Home icon to reset the map to the default view.

Use first-person and third-person views for 3D wireless maps

You can use the first-person and third-person views to gain different perspectives of your wireless network.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

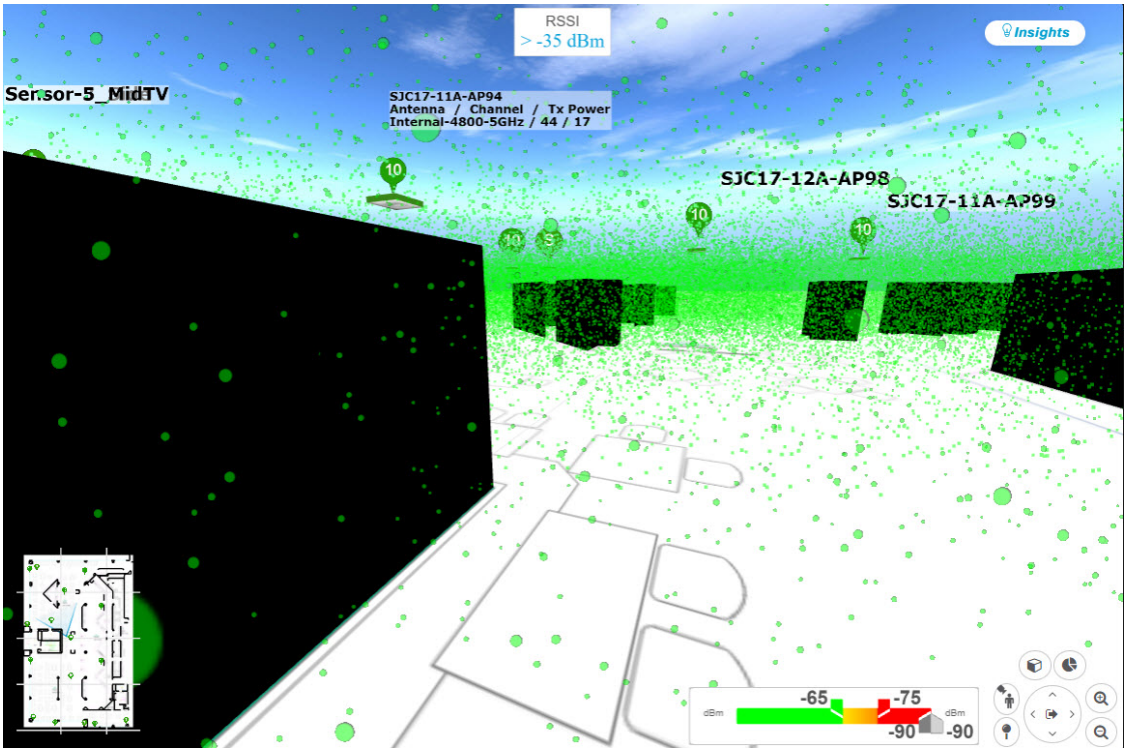
Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 To use the first-person view, click the first-person view icon  in the map navigation controls. Optionally, you can drag and drop the person icon  to a specific location on the map.

The map view changes to the first-person view.

Figure 18: First-person view



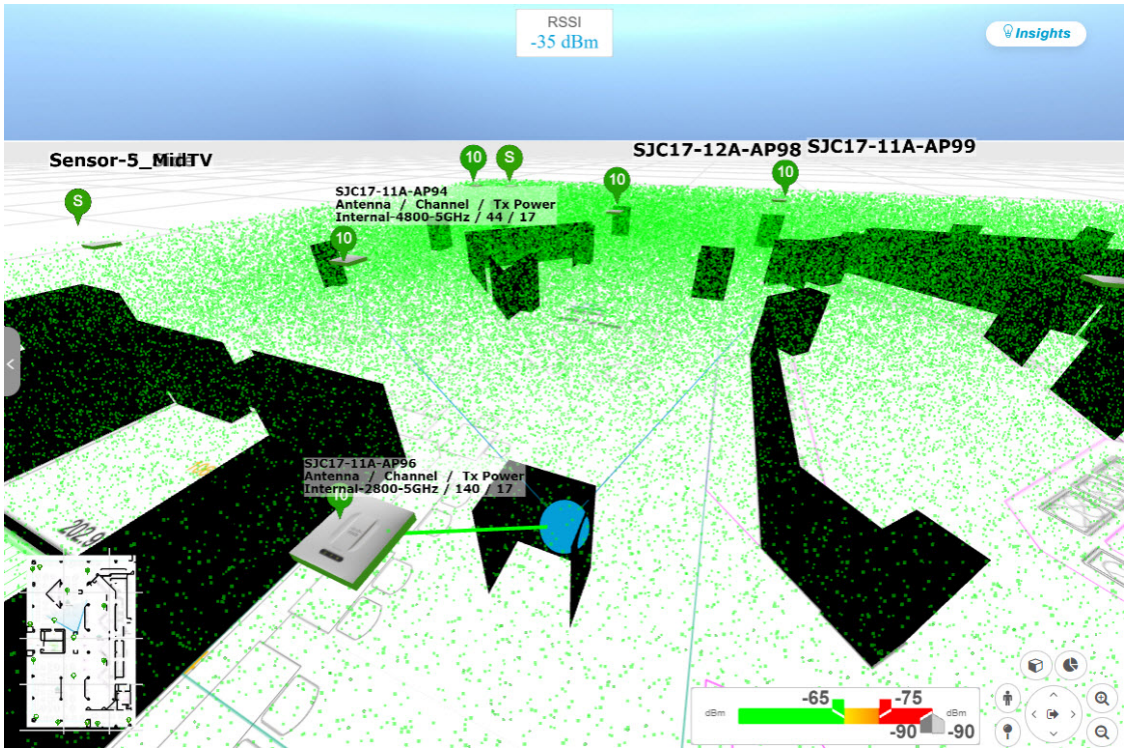
Step 5 To control the first-person view:

Action	Controls
Move forward/backward and right/left.	Use the **W**, **A**, **S**, and **D** keys or arrow keys.
Change the camera angle.	Click and hold the left mouse button on the map and move the mouse wheel.
Raise the altitude of the camera angle.	Hold the **Spacebar**.
Lower the altitude of the camera angle.	Hold **Shift** + **Spacebar**.

Step 6 To use the third-person view, click the third-person view icon  from the map navigation controls.

The map view changes to the third-person view.

Figure 19: Third-person view



Step 7 To control the third-person view:

Action	Controls
Move forward/backward and right/left.	Use the **W**, **A**, **S**, and **D** keys or arrow keys.
Change the camera angle.	Click and drag on the map.
Raise the altitude of the camera angle.	Hold the **Spacebar**.
Lower the altitude of the camera angle.	Hold **Shift** + **Spacebar**.

Step 8 To return to the default view, click the return home icon .

Display details about APs and clients

Use this procedure to view the locations of clients on a floor if you have a location service, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), installed on Catalyst Center.

Clients are identified as a small blue ball ( ) on the map.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

Note A 3D heatmap is delimited by its coverage area, which is the full floor width and length, by default. To specify a polygon for the heatmap boundaries, edit the **Coverage Area** field value in the 2D map view. However, these boundaries do not apply to the 2D map view because the full floor width and length are used for the 2D map view.

Step 4 To display details about an AP, click the AP.

The slide-in pane displays device details like the AP type, MAC address, AP model, software version, controller IP address, product type, AP mode (Flex/Fabric, Local, etc.), sensor mode, health score, issues count, and radio interface details like operating mode (Client Servicing or Monitoring), channel number, slot ID, channel width, Tx power, client count, channel utilization, antenna name, antenna angle, and elevation angle for the respective Wi-Fi band.

Step 5 To display information about a client, hover your cursor over the ball (client).

A line is drawn between the client and its associated AP. A dialog box is displayed with information, such as the client's IPv4 address, IPv6 IP address, RSSI value, and so on. To open the **Client 360** window, click the **Client 360** link in the dialog box.

Step 6 To display the client in a color that corresponds to its RSSI, SNR, or health score:

a) Click **View Options** > **Devices and Clients**.
b) Check the **Clients** check box.
c) Under the **Clients** check box, click **None** (default blue color), **RSSI**, **SNR**, or **Health Score**.

Step 7 To resize the ball, use the **Ball Size** slider in the **View Options** pane.

This feature helps you to view clients in cases where there are many clients or only a few. For example, in cases where there are many clients, you can make the ball smaller, and in cases where there are only a few clients, you can make the ball larger.

Gain insights from a 3D wireless map

Catalyst Center actively monitors the network performance of 3D wireless maps and provides insights into areas where service-level agreements (SLA) are not being met.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 At the top-right corner of the map, click **Insights**.

The **Insights** area opens and displays information about the coverage areas that don't meet a specific KPI threshold, for example, RSSI is ≥ -70 dBm.

Figure 20: Insights Area



Step 5 In the **Insights** area, you can do any of these actions:

Item	Details
View coverage gaps	Click this link to display the wireless coverage area. Red areas show where the SLA is not being met. Green areas show where it's being met.
Optimizer	Click this link to have Catalyst Center analyze the wireless coverage area. You can indicate the maximum number of APs that you are willing to move and add, and Catalyst Center computes a configuration where the wireless coverage is maximized. For more information, see Run the wireless coverage optimizer, on page 312.
Mute This Insight	Click this button to exclude an insight from displaying in the **Insights** dialog box. Muted insights appear at the bottom of the list in the **All Insights** slide-in pane.
View All Insights	Click this button to display all active and muted insights. For each insight, you can click **Mute** or **Unmute** to exclude or include its display in the **Insights** dialog box. Click **Edit Configuration** to customize the insight KPI settings. Another way to customize insight KPI settings is from the map toolbar. Hover your cursor over the gear icon in the map toolbar and choose **Insights Configurations**.

Run the wireless coverage optimizer

For wireless areas that aren't meeting their SLA, the optimizer takes your input of the maximum number of APs that you are prepared to move and add, and computes a configuration where the wireless coverage is maximized.

This procedure shows you how to run the wireless coverage optimizer.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 At the top-right corner of the map, click **Insights**.

The **Insights** area opens and displays information about the coverage areas that don't meet a specific KPI threshold, for example, RSSI is ≥ -70 dBm.

Step 5 (Optional) To display the wireless coverage area, click **View**.

Red areas show where the SLA is not being met. Green areas show where the SLA is being met.

Step 6 (Optional) If there are specific APs that you don't want the optimizer to move, you can right-click them and choose **Lock** to lock their position. To remove the lock, right-click the AP and choose **Unlock**.

Step 7 Click **Optimizer**.

Step 8 In the **Coverage Optimizer** dialog box, enter the maximum number of APs that you are prepared to move and add.

If you don't want to move or add APs, leave the corresponding field blank or enter **0**.

Step 9 Click **Run Optimizer**.

If needed, you can manually move any of the APs to other locations.

Step 10 When the analysis is complete, click **View Results**.

Catalyst Center displays a proposed layout that increases the wireless coverage to maximize the SLA. If the optimizer recommends moving an AP, the new layout displays a blue line to the recommended new location. Any new APs that have been added to the layout are displayed as blue markers ( ).

Step 11 To save the new layout as a simulation, click **Save as a plan**. To exit without saving, click the **x** at the top-right corner of the map.

Later, if you implement the recommended changes to your physical wireless network, you can save the simulation as an operational map. For information, see Create simulations for 3D wireless maps, on page 313.

Create simulations for 3D wireless maps

You can create simulations for 3D wireless maps.

Note Simulation mode is available only in 3D maps, not in 2D maps.

Simulations allow you to change device configurations without actually implementing them. You can create multiple simulations and load them at any time.

Procedure

Step 1 From the main menu, choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 In the map toolbar, click the **Simulation** toggle button to view the map in simulation mode.

The lower map toolbar displays the message: "You are in Simulation Mode".

Step 5 In the map toolbar, click **Edit/Clone**.

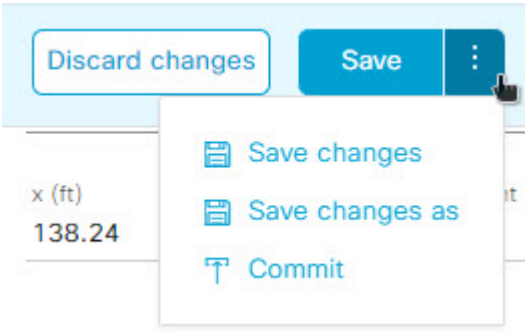
In simulation mode, only particular attributes are editable for previewing the impact of changes on the heatmap.

Step 6 Make any changes to the devices, as needed, for the simulation, and then click **Apply**.

- **APs**: You can change the model, channel, antenna, and more.
- **PAPs**: You can change the model, channel, antenna, and more.

Step 7 In the map toolbar, hover your cursor over the vertical ellipsis and choose **Save changes as** to save the configuration as a new simulation.

Figure 21: Saving as a simulation



Note Choose **Save changes** when you want to saves any changes to an existing simulation.

Choose **Commit** when you want to commit the simulation to the production environment. Note that you can only commit planned APs.

Step 8 In the **Save Simulation** dialog box, enter a name for the simulation and click **Save**.

The new simulation is displayed on the map.

Step 9 (Optional) To display a different simulation:

a. Make sure that you are in simulation mode and are not editing any devices.

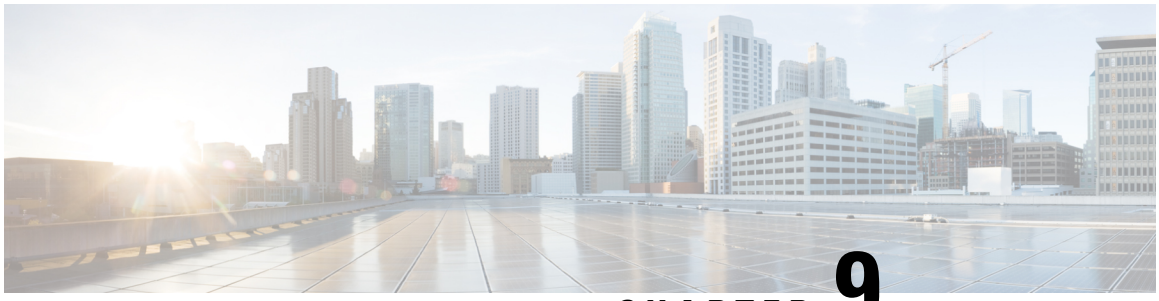
b. From the **Select Simulation** drop-down list, choose a simulation.

If you have no saved simulations, **None available** is displayed instead of the **Select Simulation** drop-down list.

Step 10 (Optional) To delete a simulation:

a. From the **Select Simulation** drop-down list, choose a simulation.

b. Click the delete icon next to the **Select Simulation** drop-down list.



CHAPTER 9

Configure Network Settings

- Network settings overview, on page 317
- Configure the time zone for a site, on page 318
- Configure the message of the day, on page 318
- Add Cisco ISE or other AAA servers, on page 319
- Configure global network servers, on page 321
- Configure global device credentials, on page 323
- Configure IP address pools, on page 337
- Configure service provider profiles, on page 350
- Configure global wireless settings, on page 350
- Configure a certificate revocation check, on page 451

Network settings overview

You can create network settings that become the default for your entire network. There are two primary areas from which you can define the settings within your network:

- **Global settings**: Settings defined here affect your entire network and include settings for servers such as DHCP, DNS, AAA, NTP, and so on; IP address pools; Device Credential profiles; Telemetry settings such as Syslog, Traps, and NetFlow.
- **Site settings**: Settings define here override global settings and can include settings for servers, IP address pools, and device credential profiles.

Note Changes in network settings that are being used by the active fabric are not supported. These network settings include site hierarchy, renaming IP pools, and several other features.

Note Certain network settings can be configured on devices automatically using the Device Controllability feature. When Catalyst Center configures or updates devices, the transactions are captured in the Catalyst Center audit logs. You can use the audit logs to help you track changes and troubleshoot issues.

You can define these global network settings by choosing **Design** > **Network Settings** and clicking the appropriate tab.

- Network servers, such as AAA, DHCP, and DNS: For more information, see Configure global network servers, on page 321.
- Device credentials, such as CLI, SNMP, HTTP, and HTPS: For more information, see Configure global device credentials, on page 323.
- IP address pools: For more information, see Configure IP address pools, on page 337.
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles: For more information, see Configure global wireless settings, on page 350.
- Configure global telemetry settings, such as syslog, SNMP, and NetFlow Collector servers using telemetry.

Configure the time zone for a site

A site's time zone is used primarily for scheduling tasks, like assigning a device to a site, provisioning, or updating telemetry settings.

When scheduling a task for a later time, the site's assigned time zone will be used by default.

To configure the time zone for a site:

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Servers** tab.

Step 3 From the left hierarchy tree, select your desired site.

Step 4 In the **Time Zone** section, choose your desired time zone from the drop-down list.

Step 5 Click **Save**.

Configure the message of the day

The message of the day is the greeting message that displays when logging into a device’s CLI. This message applies only to routers, switches, and hubs.

To configure the message of the day:

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Servers** tab.

Step 3 From the left hierarchy tree, select your desired site.

Step 4 In the **Message of the Day** section, choose one of these options:

- **Use device's existing message**

  This is the default option.

- **Set custom message**

  You can enter your own message, but the message must adhere to these constraints:

  - Cannot contain "#" or "<"
  - Cannot contain "MLTCMD" or "mltcmd"
  - Maximum line length: 80 characters
  - Maximum number of lines: 40

Step 5 Click **Save**.

Add Cisco ISE or other AAA servers

You can define Cisco Identity Services Engine (ISE) servers or other, similar AAA servers for network, client, and endpoint authentication at the site or global level. For network authentication, RADIUS and TACACS protocols are supported. For client and endpoint authentication, only RADIUS is supported. Only one Cisco ISE is supported per Catalyst Center.

You can configure the source interface under the RADIUS or TACACS server group to support multi-ISE configuration, wherein each Cisco ISE cluster has its own server group. The interface that Catalyst Center uses as the management IP is configured as the source interface for RADIUS and TACACS servers.

After you configure a Cisco ISE server for a site, the assigned devices are automatically updated on the corresponding Cisco ISE server with a /32 mask. Any changes you make to these devices in Cisco ISE are also sent to Catalyst Center automatically.

In a FIPS mode deployment, the shared secret includes a shared secret, a keywrap, and a message authenticator code key.

Before you begin

- You must have Read permission on **Advanced Network Settings**.
- You must specify the servers that authenticate Catalyst Center users in **System** > **Settings**. For more information, refer to "Configure authentication and policy servers" in the Cisco Catalyst Center Administrator Guide.
- For Cisco TrustSec (CTS) data download over HTTPS, ensure all of these prerequisites are met:
  - Cisco ISE version: Release 3.5 Patch 1 or later with HTTPS service enabled.
  - Cisco IOS XE version: Release 26.1.1 or later.
  - Supported device platforms:
    - Cisco Catalyst 9000 Series Virtual Switches

- Cisco Catalyst 9200, 9300, 9400, 9500, and 9600 Series Switches
- Cisco Catalyst 9800 Series Wireless Controllers
- Cisco Catalyst 9800 Wireless Controllers for Cloud
- Cisco Catalyst IE9300 Rugged Series
- Cisco Catalyst IE3400 Heavy Duty Series
- Cisco Catalyst IE3400 Rugged Series
- Cisco Catalyst IE3500 Rugged Series
- Cloud Edge
- Cisco 4000 Series Integrated Services Routers
- Cisco C9350 Series Smart Switches
- Cisco C9610 Series Smart Switches

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Servers**.

Step 2 Expand the **AAA** area.

Step 3 Check the **Add AAA servers** check box under **Network** and/or **Client/Endpoint** tabs and configure servers and protocols for the AAA server.

Step 4 Choose the **Server Type** for authentication and authorization: **ISE** or **AAA**.

a) If you choose **ISE**, do this configuration:

- Choose the **Protocol**: **RADIUS** or **TACACS**.
- From the **PAN** drop-down list, choose the IP address of the Cisco ISE server. The **PAN** drop-down list contains all the IP addresses of the Cisco ISE servers that are registered on the **System** > **Settings** window. Selecting a Cisco ISE IP populates the primary and secondary IP address drop-down lists with Policy Service Node (PSN) IP addresses for the selected Cisco ISE. You can either enter an IP address for the AAA server or choose the PSN IP address from the **Primary Server** and **Secondary Server** drop-down lists.
- If you choose **RADIUS**, Catalyst Center provisions the selected Cisco ISE IP addresses for Change of Authorization (CoA). Catalyst Center configures the pxGrid, PSN, and PAN IP addresses in the dynamic-authorization list for CoA operations.
- If you choose **TACACS**, check the **Single Connection** check box to minimize the number of TCP connections opened for duplicate transactions.



Note AAA settings for a physical and managed site for a particular wireless controller must match, or provisioning fails.

- Under **Cisco TrustSec (CTS) Policy and Data Download**, check the **Enable HTTPS downloads** check box to enable CTS policy and data download over HTTPS.

Note

- After you enable or disable HTTPS downloads for CTS, reprovision the devices assigned to the site. This action pushes the CTS configurations.
- If security service insertion is enabled on a fabric site, you must delete the security service insertion configuration to disable CTS policy and data download over HTTPS. For more information, refer to Delete a service insertion site, on page 1169.

b) If you choose **AAA**, do this configuration:

- Choose the **Protocol**: **RADIUS** or **TACACS**.
- From the **Primary Server** drop-down list, choose an IP address for the AAA server. Click the + icon and choose an IP address from the **Secondary Server** drop-down list. Click icon to delete the server.

  These drop-down lists contain the non-Cisco ISE AAA servers registered on the **System** > **Settings** window.

  Ensure that the AAA server IP address is not part of an existing Cisco ISE cluster.
- If you choose **TACACS**, check the **Single Connection** check box to minimize the number of TCP connections opened for duplicate transactions.

Note If you switch the **Server Type** from ISE (with TACACS) to AAA with TACACS, TACACS will be disabled on the Cisco ISE server because it is no longer used for authentication.

Step 5 Click **Save**.

Configure global network servers

You can define the global network servers that become the default for your entire network.

Note You can override the global network settings on a site by defining site-specific settings.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Servers** tab.

Step 3 Expand the **DHCP** area. Specify one or more dedicated Dynamic Host Configuration Protocol (DHCP) servers for managing the client device networking configuration.

Step 4 Check the **Add DHCP servers** check box to view the fields.

Step 5 In the **IP Address** field, enter the IP address of a DHCP server. Click the icon to add an IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

You must define at least one DHCP server in order to create IP address pools.

Step 6 Expand the **DNS** area to configure your network domain name, and specify Domain Name System (DNS) servers for hostname resolution.

Step 7 Check the **Set a domain name** check box to enter the domain name of a DNS server.

Step 8 Check the **Add DNS servers** check box to enter the IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

You must define at least one DNS server in order to create IP address pools.

Step 9 Expand the **NTP** area to specify one or more Network Time Protocol (NTP) servers to facilitate system clock synchronization for your network.

Step 10 Check the **Add NTP servers** check box to view the fields.

Step 11 In the **IP Address** field, enter the IP address of an NTP server. Click the icon to add an IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

Step 12 Click **Save**.

Configure global device credentials

"Global device credentials" refers to the common CLI, SNMP, and HTTPS credentials that Catalyst Center uses to discover and collect information about the devices in your network. Catalyst Center uses global credentials to authenticate and access the devices in a network that share these configured device credentials.

Configure global device credentials workflow

To configure global device credentials onto devices in a network, follow these high-level steps:

1. Create the global device credential. See Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, Add global SNMPv3 credentials, on page 325, and Add global HTTPS credentials, on page 327.
2. Assign the global device credential to a site. See Assign device credentials to sites, on page 329.
3. Apply the global device credential to all the devices in the selected site. See Apply device credentials to site devices, on page 331.
4. Manage the global device credential. See Manage global device credentials, on page 330.

Add global CLI credentials

You can add and save up to 10 global CLI credentials.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose a site.

Step 4 Do one of these tasks:

- If you haven't created any credentials yet, click **Create Credentials**.
- If you have created credentials, click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **CLI**.

Step 6 Complete the listed fields using this table:

Table 41: CLI credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.

Field	Description
Password	Password that is used to log in to the CLI of the devices in your network. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 (Optional) Check the **Assign credential to site** check box to assign the CLI credential to the selected site.

Step 8 Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus will display the credential.

Add global SNMPv2c credentials

You can add global SNMPv2c credentials to monitor and manage your network devices.

Note Catalyst Center does not support SNMPv2c device credentials when FIPS mode is enabled. You must specify SNMPv3 credentials instead.

Before you begin

You must have the SNMP information for your network.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose a site.

Step 4 Do one of these tasks:

- If you haven't created any credentials yet, click **Create Credentials**.
- If you have created credentials, click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **SNMPv2c Read** or **SNMPv2c Write**.

Step 6 Complete the listed fields using this table:

Table 42: SNMPv2c credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 (Optional) Check the **Assign credential to site** check box to assign the SNMPv2c credential to the selected site.

Step 8 Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus will display the credential.

Add global SNMPv3 credentials

You can add global SNMPv3 credentials to monitor and manage your network devices.

Before you begin

You must have your network's SNMP information.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose a site.

Step 4 Do one of these tasks:

- If you haven't created any credentials yet, click **Create Credentials**.
- If you have created credentials, click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **SNMPv3**.

Step 6 Complete the listed fields using this table:

Table 43: SNMPv3 credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name that is associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of these modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth Type	Authentication type to be used. (This field displays if you select **Authentication and Privacy** or **Authentication, No Privacy** as the authentication mode.) Choose one of these authentication types: • **SHA**: Authentication based on HMAC-SHA • **SHA256**: Authentication based on HMAC-SHA256. • **MD5**: Authentication based on HMAC-MD5 **Note** • The MD5 authentication type is not recommended. • Catalyst Center does not support device provisioning if only MD5 authentication type is configured on the device for software image version 17.14.1 and later. If you wish to use MD5 authentication, it is recommended to configure SHA authentication as well for Catalyst Center to discover and manage devices running on software image 17.14.1 and later.
Privacy Type	Privacy type to be used. (This field displays if you select **Authentication and Privacy** as the authentication mode.) Choose one of these privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **AES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **AES256**: 256-bit CBC mode AES for encryption on Cisco devices. • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. **Note** The DES privacy type is disabled and not supported.

Field	Description
Auth Password	SNMPv3 password that is used for gaining access to information from devices that use SNMPv3. (This field displays if you select **Authentication and Privacy** or **Authentication, No Privacy** as the authentication mode.) These passwords (or passphrases) must be at least eight characters in length and cannot contain spaces or angle brackets (< >). **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. (This field displays if you select **Authentication and Privacy** as the authentication mode.) Passwords (or passphrases) must be at least eight characters long and cannot contain spaces or angle brackets (< >). **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 (Optional) Check the **Assign credential to site** check box to assign the SNMPv3 credential to the selected site.

Step 8 Click **Save**.

A success message displays in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus displays the credential.

Add global HTTPS credentials

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, choose a site.

Step 4 Do one of these tasks:

- If you haven't created any credentials yet, click **Create Credentials**.
- If you have created credentials, click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Add** drop-down list, choose **HTTP(S) Read** or **HTTP(S) Write**.

Step 6 Complete the listed fields using this table:

Table 44: HTTP and HTTPS credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Field	Description
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain between 7 and 128 characters, including at least one of these characters: • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – **Note** The password cannot contain spaces or angle brackets (< >). Some Cisco IOS XE devices do not allow a question mark (?).

Step 7 (Optional) Check the **Assign credential to site** check box to assign the HTTPS credential to the selected site.

Step 8 Click **Save**.

A success message is displayed in the bottom-right corner. You can view the credential in the **Manage Credentials** slide-in pane. However, if you didn't assign the credential to a site, only the **System** focus displays the credential.

Assign device credentials to sites

You can assign global device credentials to a specific site or all the sites in the hierarchy. If you choose **Global**, all sites under **Global** inherit its assigned global device credentials.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, select the required site.

Step 4 Locate the type of global device credential that you want to assign.

Step 5 Check the corresponding **Assign** check box for the credential.

Step 6 From the **Credential** drop-down list, choose the credential that you want to assign to the selected site.

Step 7 Click **Save**.

The confirmation dialog box displays. Do one of these tasks:

- If you're ready to apply the device credential to the site's devices, click **Yes** and proceed to Apply device credentials to site devices, on page 331.
- If you're not ready to apply the device credential to the site's devices, click **No**.
- If there are no devices in the site, click **OK**. You can apply device credentials to the site's devices after you've added devices to the site.

Step 8 To unassign a device credential from a site:

a. From the left hierarchy tree, choose the required site.

b. Uncheck the **Assign** check box for the device credential that you want to unassign.

c. Click **Save**.

d. In the confirmation dialog box, click **Yes** to proceed with unassigning the credential from the selected site or click **No** to keep the credential assigned to the selected site.

If you chose **Yes**, a successful dialog box is displayed, indicating that the updated site may not be in sync with the device credential applied to the site's devices. Do one of these tasks:

- If you're ready to apply the device credential to the site's devices, click **Yes** and proceed to Apply device credentials to site devices, on page 331.
- If you're not ready to apply the device credential to the site's devices, click **No**.
- If there are no devices in the site, click **OK**. You can apply device credentials to the site's devices after you've added devices to the site.

Note Unassigning a device credential from a site doesn't change the credential currently applied to all the devices in that site. To update the device credential on all the devices in a site, see Update device credentials on devices, on page 336.

Manage global device credentials

You can manage global device credentials in the **Manage Credentials** slide-in pane. Depending on the focus of the data (**Current site** or **System**), you can perform specific actions to manage your global device credentials. The **Current site** focus displays only global device credentials that are assigned to the selected site. In this focus, you can add and apply global device credentials to only the currently selected site. The **System** focus displays the system's pool of global device credentials. In this focus, you can add, edit, and delete global device credentials. Also, from this focus, you can apply a device credential to all the sites in the hierarchy.

Apply device credentials to site devices

With the **Focus** drop-down list, you can apply a global device credential either to devices in all sites or a specific site. If you apply a device credential using the **System** focus, Catalyst Center checks if any of the sites in the hierarchy are assigned to use this device credential. Then it pushes the change to those devices. If you apply a device credential using the **Current site** focus, Catalyst Center checks if the currently selected site and its child sites are assigned to use this device credential. Then it pushes the change to those devices.

Use this procedure to apply a device credential either to the devices in all sites or to the devices in a specific site.



Note You can apply only CLI, SNMP v2c Read, SNMP v2c Write, and SNMPv3 credentials to the devices in a site. Catalyst Center doesn't support the application of HTTPS Read and HTTPS Write credentials to the devices in a site.

Before you begin

Make sure that you assigned the device credential (that you want to apply) to the required sites. For more information, see Assign device credentials to sites, on page 329.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, select the required site.

Step 4 Click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose a focus (**Current site** or **System**) to define where you want to apply the credential.

Step 6 In the credential's corresponding **Actions** column, hover your cursor over **…** and choose **Apply**.

Step 7 If you are applying a CLI credential, decide how you want to apply this credential to the devices in a site and then click **Next**. Otherwise, proceed to Step 8, on page 332.

If you...	Then...
• check both the **Push credential to devices** and **Verify authentication on devices** check boxes, or • check the **Push credential to devices** check box and uncheck the **Verify authentication on devices** check box	Catalyst Center will update the CLI credential locally on the affected devices (which includes performing provisioning and validation checks) and update the CLI credential stored in inventory for affected devices. **Note** The deployment of this configuration may take some time to complete.

If you...	Then...
uncheck the **Push credential to devices** check box and check the **Verify authentication on devices** check box	Catalyst Center will only verify authentication on the affected devices and update the CLI credential stored in inventory for affected devices. **Note** We recommend this configuration for devices using AAA or Cisco ISE authentication management.
uncheck both the **Push credential to devices** and **Verify authentication on devices** check boxes	Catalyst Center will only update the CLI credential stored in inventory for affected devices. **Note** • Only uncheck the **Verify authentication on devices** check box if the devices in a site are unreachable or inaccessible. • If the **Verify authentication on devices** check box is unchecked and the CLI credentials are incorrect when applied to affected devices, these devices might enter the Unmanaged state on the **Provision** > **Inventory** window.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Reschedule the application of device credentials

If you want to reschedule a device credential task (applying the device credential to a site's devices), use this procedure.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 Do one of these tasks:

- If you used the **Current site** focus when you applied the device credential, choose the same site from the left hierarchy tree that you applied the device credential to.

- If you used the **System** focus when you applied the device credential, proceed to Step 4, on page 333.

Step 4 Click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose the same focus that you used to apply the device credential.

Step 6 In the **Manage Credentials** table, locate the device credential with the scheduled application that you want to reschedule.

Step 7 In the device credential's corresponding **Actions** column, hover your cursor over **...** and choose **Reschedule**.

Note If **Reschedule** is not displayed and instead **Apply** is displayed, make sure that you chose the same focus and same site as you did in the scheduled application of the device credential. Clicking **Apply** creates a new task; it doesn't reschedule the existing task.

Step 8 Reschedule the date and time of the task, and then click **Apply**.

Note You cannot change the time zone.

A success message is displayed in the bottom-right corner, indicating that the device credential was successfully rescheduled.

View the status of a device credential

With the **Current site** focus on the **Manage Credentials** slide-in pane, you can view the status of a device credential.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 From the left hierarchy tree, select the required site.

Step 4 Click **Manage Credentials**.

Step 5 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose **Current site**.

Step 6 In the **Manage Credentials** table, locate the relevant credential.

Step 7 In credential's corresponding **Status** column, view the credential's status.

One of these statuses display:

- **Synced**: The device credential assigned to selected site matches the device credential applied to the selected site’s devices.
- **Not Synced**: The device credential assigned to selected site doesn’t match the device credential applied to the selected site’s devices.

- **Date and time**: This is the scheduled date and time of the device credential's application. For example, Feb 1, 2024 9:00 AM.
- **Partial Success**: The application of the device credential was partially successful.
- **Failed**: Catalyst Center failed to apply the device credential to at least one of the devices assigned to the selected site.
- **Not Applicable**: The device credential is not supported by any of the site's devices.
- **—**: The device credential cannot be applied because either the site has no devices or the child sites use a different credential of the same credential type.

Hover your cursor over the credential's status to view additional details.

Tip To view the latest status in the system, click the refresh icon in the top-right corner of the table.

Step 8 Alternatively, navigate to the **Provision** > **Inventory** window.

The **Credential Status** column displays one of these statuses:

- **Success**: Catalyst Center successfully applied the credential change.
- **Failed**: Catalyst Center was unable to apply the credential change. Click **See Details** to view additional information about which credential change failed and why.
- **Not Applied**: The device credential applied to the selected site's device does not match the device credential assigned to the selected site.
- **Not Applicable**: The device credential is not applicable to the device type.

If you edited and saved more than one credential (for example, CLI, SNMP, and HTTPS), the **Credential Status** column displays **Failed** if Catalyst Center was unable to apply *any* of the credentials. Click **See Details** to display additional information about which credential change failed.

Guidelines for editing global device credentials

These are guidelines and limitations for editing existing global device credentials:

- Catalyst Center uses this process when you edit, save, and then apply a global device credential:
  1. Catalyst Center pushes the credential to the device that has local authentication. With local authentication, credential changes are applied and Catalyst Center manages the devices using these credentials.

     (Catalyst Center does not push CLI credential changes to a device that is under a site with an inherited or configured AAA server. With AAA authentication, credential changes are not applied. Catalyst Center manages the devices using these credentials only if the same credentials exist on the AAA server.)
  2. After successfully pushing the credential to the device, Catalyst Center confirms it can reach the device using the new credential.

Note If this step fails, Inventory uses the old credentials to manage the device even though Catalyst Center pushed the new credentials to the device. In this case, the **Provision** > **Inventory** window might indicate that the device is Unmanaged if you updated an existing credential.

3. After successfully reaching the device using the new credential, the Catalyst Center Inventory starts managing the device using the new credential.

- Sites can contain devices that use SNMPv2c and SNMPv3 credentials. When you edit, save, and apply global SNMPv2c or SNMPv3 credentials, Catalyst Center pushes those changes to devices and enables the credentials. For example, if you have a device that uses SNMPv2c, but you edit, save, and apply the SNMPv3 global credential, Catalyst Center pushes the new SNMPv3 credential to all devices in the associated site and enables it. This means that all devices will be managed using SNMPv3, even the devices that previously had SNMPv2c enabled.
- To avoid any possible disruptions, modify the **User Name** when you edit CLI credentials. This creates a new CLI credential and leaves any existing CLI credentials unchanged.

Edit global device credentials

You can edit and save global device credentials without Catalyst Center applying those credential changes until you're ready. (For more information about applying device credentials, see Apply device credentials to site devices, on page 331.) If you edit a device credential that was previously applied to a site's devices, the device credential status displays **Not Synced** for all the sites that use this device credential. This status displays because the device credential assigned to the site no longer matches the device credential applied to that site's devices.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Device Credentials** tab.

Step 3 Click **Manage Credentials**.

Step 4 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose **System**.

Step 5 In the **Manage Credentials** table, locate the credential that you want to edit.

Step 6 In the credential's corresponding **Actions** column, hover your cursor over **...** and choose **Edit**.

Step 7 In the confirmation dialog box, click **OK** to proceed with editing this credential.

Note If this credential is assigned to other sites, any changes to this credential will impact those sites.

Step 8 In the slide-in pane, make the required changes and then click **Save**.

A success message displays in the bottom-right corner, indicating that the device credential was successfully updated.

Note The CLI password credentials support only *ASCII-printable characters* (character code 32-127; see https://en.wikipedia.org/wiki/ASCII#Printable_characters).

Delete device credentials

If you want to delete a device credential, consider first if the device credential is assigned to any sites. If it's not assigned to any sites, you can simply delete the device credential from the system's pool of global device credentials using the **System** focus. If it's assigned to any sites, you must first either unassign the device credential from all sites that use it or delete those sites. Then you can delete the device credential from the system's pool of global device credentials.

Note Deleting a device credential only removes it from the system's pool of global device credentials. Catalyst Center never removes any credentials from devices.

Before you begin

If the device credential that you want to delete is assigned to any sites, you must first either unassign the device credential from all the sites that use it or delete those sites. For more information, see Create, edit, and delete a site, on page 240 or Step 8, on page 330 in Assign device credentials to sites, on page 329.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**

Step 2 Click the **Device Credentials** tab.

Step 3 Click **Manage Credentials**.

Step 4 In the **Manage Credentials** slide-in pane, from the **Focus** drop-down list, choose **System**.

Step 5 In the **Manage Credentials** table, locate the credential that you want to delete.

Step 6 In the credential's corresponding **Actions** column, hover your cursor over **…** and choose **Delete**.

Step 7 In the **Warning** dialog box, click **Yes**.

A success message is displayed in the bottom-right corner, indicating that the device credential was successfully deleted.

Update device credentials on devices

When a device credential is unassigned from a site, the credential currently applied on that site’s devices isn't automatically updated. The devices retain the existing credential until a new one is applied, so the device always has credentials configured. You can update the device credentials on all the devices in a site using these high-level steps.

Procedure

Step 1 Unassign the device credential from the required site. See Step 8, on page 330 in Assign device credentials to sites, on page 329.

Step 2 Assign the new device credential to the same site. See Assign device credentials to sites, on page 329.

Alternatively, you can unassign and assign in one step by clicking **Save** on the **Device Credentials** window.

Step 3 Apply the new device credential to that site's devices. See Apply device credentials to site devices, on page 331.

Step 4 Alternatively, you can log in to the device and manually update the device credential.

Configure IP address pools

Catalyst Center supports IPv4 and IPv6 dual-stack IP pools.

You can manually create IPv4 and IPv6 address pools.

You can create IPv6-only pools at the global level and reserve them at the site level.

You can also configure Catalyst Center to communicate with an external IP address manager. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Click **Add IP Pool** and complete the required fields in the **Add IP Pool** slide-in pane:

- **IP Pool Name**: Unique name for the IP address pool.
- **Type**—Type of IP address pool:
  - **LAN**: Used to assign IP addresses to LAN interfaces for applicable underlays. Choose this option for LAN automation.
  - **Management**: Used to assign IP addresses to management interfaces.
  - **Service**: Used to assign IP addresses to service interfaces.
  - **WAN**: Used to IP addresses to WAN interfaces.
  - **Tunnel:** : Used to assign IP addresses to site-to-site VPN for IPsec tunneling.
  - **Generic**: Used for all other network types.
- **IP Address Space**: Choose **IPv4** or **IPv6** to create an address pool.
- **IP Subnet** : Specify the range and structure of IP addresses that the pool will manage and allocate.

- **Prefix length**: IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses.
- **Gateway**: Gateway IP address.
- **DHCP Server(s)**: IP address of the DHCP servers associated with this IP pool.
- **DNS Server(s)**: IP address of the DNS servers associated with this IP pool.

If you have configured Catalyst Center to communicate with an external IP address manager, you can't create an IP pool that overlaps an existing IP address pool in the external IP address manager.

Step 3 Click **Save**.

The newly added pool displays in the **IP Address Pools** table. You can click the **IPv4** tab or **IPv6** tab in the **Subnet Type** area to view only the IPv4 or IPv6 address pools.

Note When you edit an IP address pool and make DHCP changes, you don't need to reprovision the device that uses the IP address pool. However, if a fabric device uses the updated IP address pool, you must reconfigure the fabric to which the device is associated. For more information, refer to Reconfigure a fabric, on page 1031.

Import IP address pools from an IP address manager

You can import IP address pools from Bluecat or Infoblox.

Note The IP address pools cannot have subpools or any assigned IP addresses.

You must configure Catalyst Center to communicate with an external IP Address Manager (IPAM). For more information, see the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the **Import** drop-down list, choose **Import from IPAM Server**.

Step 3 In the slide-in pane, enter a CIDR and then click **Retrieve** to get the list of IP pools available to import.

Step 4 Click **Select All** or choose the IP address pools to import.

Step 5 Click **Import**.

Pools will be imported at the Global site.

Import IP address pools from a CSV file

You can import IP address pools from a CSV file.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the **Import** drop-down list, choose **Import from CSV File**.

Step 3 Click **Download sample template** to download the latest sample file.

Step 4 Add the IP address pools to the file and save the file to your local machine.

Step 5 Upload the CSV file by doing one of these actions:

a) Drag and drop the file into the drag and drop area.

b) Click **Choose a file** and then select the file from your local machine.

Step 6 Click **Import**.

Pools will be imported at the Global site.

Reserve an IP address pool

Before you begin

Ensure that one or more IP address pools have been created at the Global site.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, select the required site.

Step 3 Click the **Reserve IP Pool** link.

Step 4 In the **Reserve IP Pool** slide-in pane, complete these fields to reserve all or part of an available global IP address pool for the selected site:

- **IP Pool Name**: Unique name for the reserved IP address pool.
- **Type**—Type of IP address pool:
  - **LAN**: Intended for the assignment of IP addresses to LAN interfaces for applicable underlays. Choose this option for LAN automation.
  - **Management**: Intended for the assignment of IP addresses to management interfaces.
  - **Service**: Intended for the assignment of IP addresses to service interfaces.
  - **WAN**: Intended for the assignment of IP addresses to WAN interfaces.
  - **Generic**: Used for all other network types. This is the default option.

- **IP Address Space**: Check either the **IPv4** or the **IPv6** check box to create an address pool. To create a dual-stack pool, check both the **IPv4** and **IPv6** check boxes.
- **Global Pool**: Select the address pool from which you want to reserve the pool. You can enter text in the search field to filter the drop-down list's results.
- **Prefix length / Number of IP Addresses**—Specify how to choose the pool you want to reserve:

If you want to ...	Then ...
reserve a pool with a particular IP route prefix,	**a.** Click the **Prefix length** radio button. **b.** Choose the appropriate prefix length value from the drop-down list. **c.** In the **IPv4 Subnet**/**IPv6 Subnet** field, enter the subnet address you want to use.
reserve a pool containing a specific number of addresses,	**a.** Click the **Number of IP Addresses** radio button. **b.** In the **Total host** field, enter the size of the pool you want to reserve.

If you choose **/64** as the prefix length for an IPv6 IP address pool, the **SLAAC Support** check box is displayed and checked by default. When this option is selected, devices automatically acquire IP addresses without the need for DHCP servers.

- **Gateway**: Gateway IP address. This field is displayed only when the **Prefix length** radio button is selected.
- **Overlapping**: Specify whether you want to enable overlapping for the CIDR subnet of this pool:

If you ...	Then ...
don't want to allow the creation of IP pools that overlap with this pool's subnet,	ensure that the **Off** radio button is already selected, as this is the default setting.
want to allow the use of this pool's CIDR subnet,	**a.** Click the **On** radio button. **b.** Specify the address space identifier that you want to use. Either click the **Create new** radio button and enter an identifier or click the **Select existing** radio button and select an identifier from the drop-down list. **Important** Take care when you enter the name for a new address space identifier. You will not be able to change the name later.

- **DHCP Server(s)**: IP address of the DHCP servers associated with this IP pool.
- **DNS Server(s)**: IP address of the DNS servers associated with this IP pool.

Step 5 Click **Reserve**.

Important If you reserve both IPv4 and IPv6 address pools (which means that the fabric is provisioned with a dual-stack IP pool), you cannot switch back to a single-stack IPv4 pool if the IPv6 pool is already attached to a VN.

However, if the IPv6 pool is *not* attached to a VN, you can downgrade it back to a single-stack IPv4 pool by completing these steps:

a. From the **IP Address Pools** page, hover your cursor over the pool's ellipsis icon (•••) in the **Actions** column and then click **Edit**.

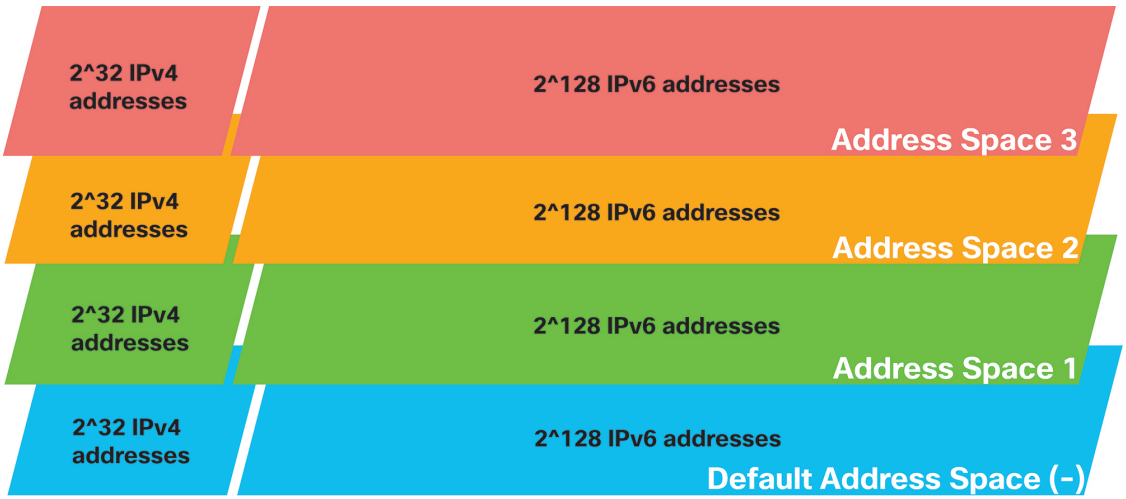
b. In the **Edit IP Pool** slide-in pane, uncheck the **IPv6** check box.

c. Click **Save**.

Overlapping IP address pools

Catalyst Center 3.1.5 supports CIDR overlapping, which provides more flexibility when assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pools to create different address spaces (as visualized in Figure 22: CIDR overlapping, on page 341).

Figure 22: CIDR overlapping



After upgrading to Catalyst Center 3.1.5, all IP address pools are placed in the default address space. By default all newly created IP pools are placed in the default address space. Each pool is mapped to a single address space and has overlapping disabled, by default. At any point after an address pool has been created, you can enable or disable overlapping—provided that it resides at level below your deployment's global site. When enabled, address pools can overlap (either partially or fully) across different address spaces.

Overlapping in Cisco SD-Access environments

In Cisco SD-Access environments, overlapping is built around the SDA_OVERLAP context key, which is pushed into the ippoolcontext table in IPAM services. Cisco SD-Access queries IPAM endpoints to filter out overlap based on this key.

Two primary types of context values are pushed for IP pools:

- SDA_VN_{VN_NAME}: This value allows for IP pool overlap across different VNs.
- SDA_GLOBAL: This value indicates that no overlap is allowed for the associated IP pools.

External IPAM integration

The support of overlapping IP address pools has been integrated with two external IP Address Management (IPAM) systems: Infoblox and BlueCat. Catalyst Center address spaces map to Infoblox Network Views and BlueCat Configurations. The names of the Network Views or Configurations created by Catalyst Center in the external IPAM system follow the format *Cisco_Overlap_<address space identifier>*. *Cisco_Overlap_* is prepended to the address space identifier used in Catalyst Center.

Catalyst Center does not support the use of overlapping IP address pools integrated with Catalyst Center through the Generic IPAM interface.

Earlier IPAM integration allowed provisioning applications (LAN Automation and SD-Access) to assign the same IP address multiple times from a pool. This feature is not visible in the IPAM user interfaces. If a third-party IPAM is integrated, it is visible from that application's user interface.

For example:

- In Infoblox, new network views are created with names starting with *CISCO_DNACenter-*.
- In BlueCat, new configurations are created with names starting with *CISCO-DNACenter-*.

These network views and configurations contain overlapping IP pools and duplicate IP addresses.

Notes and requirements for overlapping IP address pools

General

- IP address pools can overlap across different address spaces. They can't overlap within the same address space.
- Overlapping can only be enabled for IP address pools that reside at a level below your Catalyst Center deployment's Global site.
- The name for an address space identifier cannot be changed after it has been created.
- IP address pools that don't have overlapping enabled can reside in any address space.
- When creating or editing an IP address pool, you can select or create non-default address spaces. IDs for these address spaces must be unique. They can include alphanumeric characters, as well as hyphens and underscores (as long an ID doesn't start with one of these two characters).
- When an IP address pool is created, its address space assignment is fixed and cannot be changed.

Cisco SD-Access

Use this table to determine whether a particular feature combination supports overlapping IP address pools.

Feature	Segment	Multicast	Layer 3 handoff	Extranet	Sites that are connected via LISP/BGP Cisco SD-Access transit
Segment	On different VNs	On different VNs	No overlap	No overlap	No overlap between connected sites
Multicast	On different VNs	On different VNs	No overlap	No overlap	No overlap between connected sites
Infrastructure VN	No overlap	No overlap	No overlap	No overlap	No overlap
Layer 3 handoff	No overlap	No overlap	No overlap	No overlap	No overlap
Extranet	No overlap	No overlap	No overlap	No overlap	No overlap
Sites that are connected via LISP/BGP Cisco SD-Access transit	No overlap between connected sites	No overlap between connected sites	No overlap	No overlap	No overlap between connected sites

Troubleshooting overlapping IP address pools

This topic provides guidance on how to troubleshoot issues you may encounter when overlapping IP address pools are configured in your Catalyst Center deployment.

General

- IPAM service logs are the main troubleshooting resource when an overlapping issue occurs.
- Issues can arise after creating a new overlapping IP address pool that conflicts with an address pool that has overlapping disabled.
- If an existing IP address pool is visible in the UI, you can change its overlapping setting if allowed by provisioning applications.
- Some IP address pools that have overlapping disabled may be hidden because they are child pools for provisioning apps and must remain non-overlapping for them to operate properly.

Cisco Software-Defined Access

- If Catalyst Center validates subnets and IP address pools that have not been reserved yet, do the following:
  - Run this SQL query to check for unused pools that still contain the SDA_OVERLAP context (as they can cause problems):

```
SELECT *
FROM   ippoolcontext
WHERE  contextkey='SDA_OVERLAP' <= This outer query is finding all SDA_OVERLAP
```

```
context pushed
AND    ipaddresspoolinfo_id IN
       (
              SELECT id
              FROM   ipaddresspoolinfo
             WHERE  usedpercentage = '0'); <= this inner query is finding all pools
 who have 0% ussage
```

- Collect information from the following tables: ipaddresspoolinfo, ippoolcontext, and ippoolgroupinfo.

- In the SPF log files, check these items for traceability:
  - Validate overlapping IP Pools on all VNs
  - Overlapping CIDR
  - No overlapping CIDRs to report
  - cfsPoolOverlapCheck

Edit IP address pools

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, select the required site.

Step 3 To edit all the IP address pools in bulk:

a) From the **More Actions** drop-down list, choose **Edit all**.

b) In the **Warning** dialog box, click **Yes**.

c) In the **Edit IP Pools** slide-in pane, make the desired changes and click **Save**.

Step 4 To edit only specific IP address pools:

a) Check the check box next to the desired IP address pools.

b) From the **More Actions** drop-down list, choose **Edit**.

Alternatively, from the **Actions** column, hover your cursor over the ellipsis icon (•••) and click **Edit** for one of the selected IP address pools.

c) In the **Edit IP Pools** slide-in pane, make the desired changes and click **Save**.

What to do next

If the updated IP address pools are used in a fabric network, you must reconfigure the corresponding fabric on the **Provision** > **Fabric Sites** window. For more information, see Reconfigure a fabric, on page 1031.

Delete IP address pools

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, select the required site.

Step 3 To delete all the IP address pools in bulk:

a) From the **More Actions** drop-down list, choose **Delete all**.

b) In the **Warning** dialog box, click **Yes**.

Step 4 To delete only specific IP address pools:

a) Check the check box next to the desired IP address pools.

b) From the **More Actions** drop-down list, choose **Delete**.

Alternatively, from the **Actions** column, hover your cursor over the ellipsis icon (•••) and click **Delete** for one of the selected IP address pools.

c) In the **Warning** dialog box, click **Yes**.

Clone an IP address pool

You can clone an existing IP address pool at the site level. When you clone an IP address pool, the DHCP server and DNS server IP addresses are automatically filled.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, select the required site.

Step 3 Locate the desired IP address pool and, in the **Actions** area, click **Clone**.

Step 4 In the **Clone IP Pool** window, do these steps:

a) Optionally, edit the pool name. (You cannot edit the Type, IP Address Space, or Global Pool values, which are inherited from the pool from which you are cloning.)

b) Edit the CIDR prefix values as necessary.

c) Click **Clone**.

Release IP address pools

You can release single-stack and dual-stack pools that are reserved at the site level.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the left hierarchy tree, select the required site.

Step 3 To release all the IP address pools in bulk:

a) From the **More Actions** drop-down list, choose **Release all**.

b) Click **Yes** in the **Warning** message.

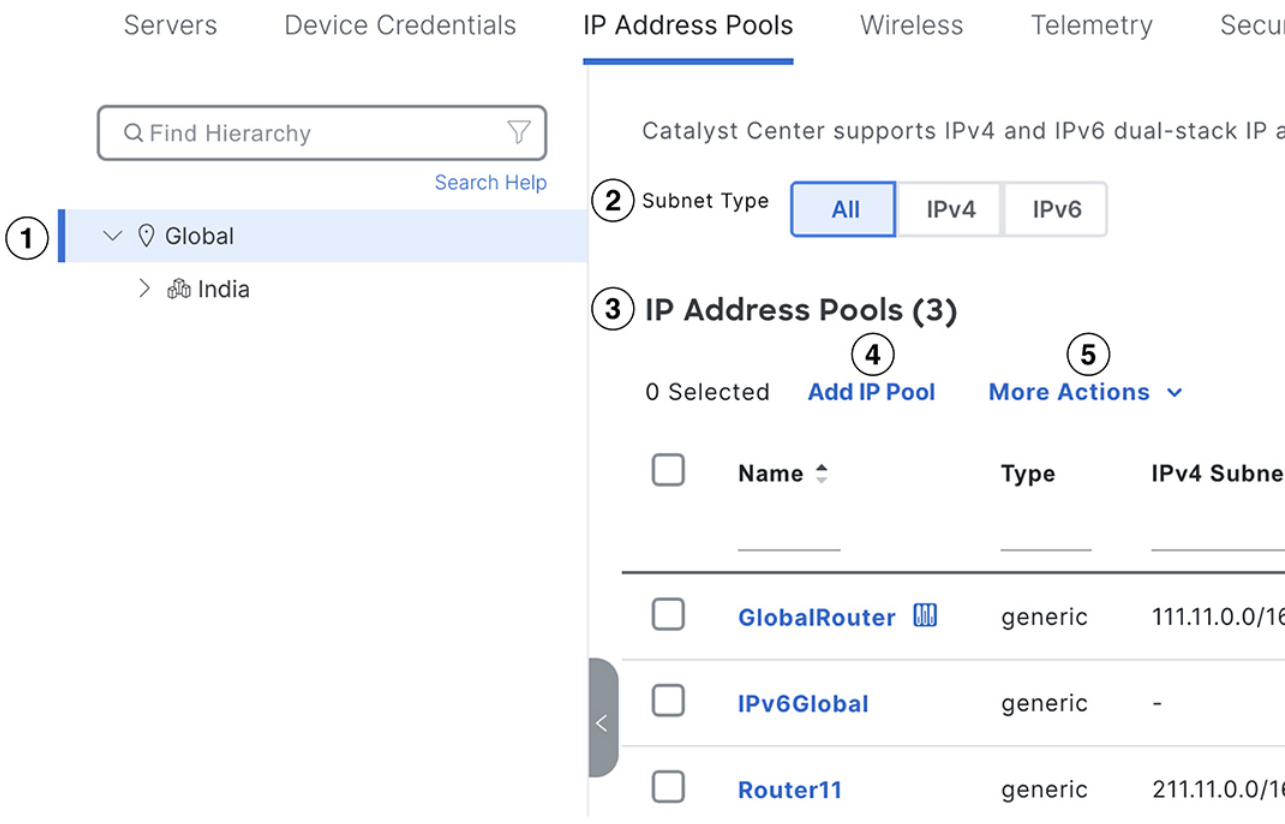
Step 4 To release only the desired IP address pools:

a) Choose the desired IP address pool(s) and from the **More Actions** drop-down list, click **Release**.

b) Click **Yes** in the **Warning** message.

View IP address pools

From the **IP Address Pools** page, you can view the IP address pools that have been configured for your Catalyst Center deployment.



The items displayed on this page will vary (as explained in these descriptions), depending on whether your entire network or a specific site is selected in the left hierarchy tree.

Table 45: Elements of the P Address Pools page

Callout	Description
1	**Left hierarchy tree**: From here, you can choose whether you want to view IP address pool information for your entire network or a particular site.
2	**Subnet type area**: From here, you can filter the IP address pools that are displayed by their configured IP version.

Callout	Description
3	**IP Address Pools table**: This table lists configured IP address pools and provides this information: • Name: Click an address pool's name to open a slide-in pane that provides more detailed information for that pool (such as the global/network-level address pool it's mapped to and the IP address of its DHCP server). • Type • IPv4 and IPv6 subnet • Percentage of IPv4 and IPv6 addresses that are currently being used **Note** To open a pop-up window that indicates how an address pool is using its available IP addresses, click its information (**i**) icon. If overlapping is enabled for the address pool, the pop-up window also indicates the number of configured overlaps. You can click the **View Overlapping details** link to open a slide-in pane that lists the percentage of assigned and unassigned IP addresses for each address space. • An indication whether overlapping is enabled (this column is only displayed when a site is selected in the left hierarchy tree) • Address space identifier: • This column is only displayed when a site is selected in the left hierarchy tree. • A hyphen indicates that an address pool resides within the default address space. • The site an address pool is inherited from: • This column is only displayed when a site is selected in the left hierarchy tree. • No value is listed if the address pool is reserved by the selected site. In the **Actions** column, you can hover your cursor over the ellipsis (**…**) and initiate one of these operations for the corresponding address pool: • **Edit**: See Edit IP address pools, on page 344 for more information. • **Delete**: This option is only displayed when your entire network is selected in the left hierarchy tree. See Delete IP address pools, on page 345 for more information. • **Clone**: This option is only displayed when a site is selected in the left hierarchy tree. See Clone an IP address pool, on page 345 for more information. • **Release**: This option is only displayed when a site is selected in the left hierarchy tree. See Release IP address pools, on page 345 for more information.

Callout	Description
4	• **Add IP Pool link**: This link is displayed when your entire network is selected in the left hierarchy tree. Click the link to open the **Add IP Pool** slide-in pane and configure the settings for a new IP address pool. See Configure IP address pools, on page 337 for more information. • **Reserve IP Pool**: This link is displayed when a site is selected in the left hierarchy tree. Click the link to open the **Reserve IP Pool** slide-in pane and specify the settings for the IP address pool that you want to reserve. See Reserve an IP address pool, on page 339 for more information.
5	**More Actions drop-down list**: Click this drop-down list to complete one of these actions: • **Edit**: Choose this option to open the **Edit IP Pool** slide-in pane and make changes to the selected IP address pool. See Edit IP address pools, on page 344 for more information. **Note** These settings are fixed and cannot be updated: • Type • IP address space • IP subnet • Prefix length • **Delete**: This option is displayed when your entire network is selected in the left hierarchy tree. Choose the option to delete the selected IP address pool. See Delete IP address pools, on page 345 for more information. • **Release**: This option is displayed when a site is selected in the left hierarchy tree. Choose the option to release the selected IP address pool that's currently reserved by this site. See Release IP address pools, on page 345 for more information. • **Edit all**: Choose this option to perform a bulk edit of every configured IP address pool. You can update the DHCP and DNS servers used by the address pools. • **Delete all**: This option is displayed when your entire network is selected in the left hierarchy tree. Choose the option to delete all of the configured IP address pools. • **Release all**: This option is displayed when a site is selected in the left hierarchy tree. Choose the option to release every IP address pool that's currently reserved by this site.
6	**View selector**: From here, you can toggle between viewing this page in table or treemap view.
7	**Import drop-down list**: Click to import IP address pool information into Catalyst Center. You can import this information from either the IPAM server your Catalyst Center deployment uses or a CSV file. This item is displayed only when your entire network is selected in the left hierarchy tree.

Callout	Description
8	**Export link**: Click to export the **IP Address Pools** table as a CSV file that you can view in applications such as Microsoft Excel. This item is displayed only when your entire network is selected in the left hierarchy tree.
9	**Take a Tour link**: Click to view pop-up windows that highlight actions you can complete from this page.
10	**Table Settings icon**: Click to open the **Table Settings** slide-in pane. From here, you can configure how the **IP Address Pools** table looks as well as the information it provides.

Configure service provider profiles

You can create a service provider profile that defines the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class service models. After you create a service provider profile, you can assign it to an application policy and to the WAN interfaces in the application policy scope, including setting the subline rate on the interface, if needed.

Procedure

Step 1 From the main menu, choose **Design** > **Service Provider Profiles**.

Step 2 If there are no existing service provider profiles, click **Create**.

Step 3 Click the plus icon.

Step 4 In the **Profile Name** field, enter a name for the service provider profile.

Step 5 In the **WAN Provider** field, enter a name for the WAN provider.

Step 6 From the **Model** drop-down list, choose a class model: **4 class**, **5 class**, **6 class**, or **8 class**.

For a description of these classes, see Service provider profiles, on page 1222.

Step 7 Click **Save**.

Note You cannot create duplicate service provider profiles.

Configure global wireless settings

Global wireless network settings include these settings:

- Service Set Identifiers (SSIDs)
- RF profiles

- Wireless interfaces and VLAN groups
- AP profiles
- FlexConnect
- Anchor groups
- Security
- Power profiles
- Antenna radio profiles
- Cisco Spaces and Cisco Connected Mobile Experiences (CMX) servers
- Remote teleworker
- 802.11be profiles

Note You can create a wireless sensor device profile for only Cisco Aironet 1800s Active Sensor devices.

You can use the **Search All Settings** field in the wireless network settings dashboard to find specific wireless network settings. You can customize the wireless network settings dashboard using **Edit Dashboard**. For more information about customizing the wireless network settings dashboard, see Customize the wireless network settings dashboard, on page 351.

Customize the wireless network settings dashboard

You can customize the wireless network settings dashboard to update the priorities of the network settings displayed in the dashboard using the **Edit Dashboard** option. Catalyst Center applies the dashboard customizations to all the sites in the wireless network settings dashboard.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Edit Dashboard**.

Step 5 In the **Customize Wireless Settings Dashboard** slide-in pane, drag and drop the required network settings to the new positions to change their priority in the dashboard.

Step 6 Click **Save**.

Create SSIDs for an enterprise wireless network

This procedure describes how to configure SSIDs for an enterprise wireless network.

Note The SSIDs are created at the global level. Sites, buildings, and floors inherit settings from the global level.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **SSIDs**.

Step 5 In the **SSID** table, hover your cursor over **Add**, and choose **Enterprise**.

Step 6 In the **Wireless SSID** workflow, complete the **Basic Settings** setup:

a) If the **Sensor** toggle button is available, ensure that it's disabled.

b) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.

c) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

d) (Optional) In the **Policy Profile Name** field, change the policy profile name.

By default, Catalyst Center automatically copies the WLAN profile name as the policy profile name.

e) (Optional) Use the **Copy to Policy Profile Name** check box for one of these options:

- Automatically copy the WLAN profile name as the policy profile name.
- Enter a different name for the policy profile.

f) In the **Radio Policy** area, do these tasks:

- Check the **2.4GHz** check box to create the WLAN for 2.4-GHz.
- Check the **5GHz** check box to create the WLAN for 5-GHz.
- Check the **6GHz** check box to create the WLAN for 6-GHz. This band is supported for devices running Cisco IOS XE Release 17.7 or later.
- From the **802.11b/g Policy** drop-down list, choose a policy.

Note This drop-down list is available only when you check the **2.4GHz** check box.

- Check the **Band Select** check box to choose the required band.

Note This check box is available only when you check both the **2.4GHz** and **5GHz** check boxes.

- Check the **6 GHz Client Steering** check box to enable client steering.

Note This check box is available only when you check the **6GHz** check box.

g) To enable or disable the fastlane capabilities on the network, use the **Fast Lane** toggle button.

By enabling fastlane, you can set the iOS devices to receive an optimized level of wireless connectivity and enhanced QoS.

When fastlane capabilities are enabled, QoS selection isn't applicable.

h) In the **Quality of Service(QoS)** area, do these tasks:

- From the **Egress** drop-down list, choose an egress QoS: **VoIP (Platinum)**, **Video (Gold)**, **Best Effort (Silver)**, or **Non-real Time (Bronze)**
- From the **Ingress** drop-down list, choose an ingress QoS: **VoIP (Platinum)**, **Video (Gold)**, **Best Effort (Silver)**, or **Non-real Time (Bronze)**

Note Ingress QoS is applicable only for Cisco IOS XE wireless controllers.

The QoS selection isn't applicable when **Fast Lane** is enabled. For Cisco IOS XE wireless controllers, QoS (both egress and ingress) is set to empty. For Cisco AireOS Wireless Controllers, the egress QoS is set to **VoIP (Platinum)**.

i) Under **SSID STATE**, use the toggle buttons to enable or disable these settings:

- **Admin Status**: Use this toggle button to turn on or turn off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and are accessible, and the APs still require licenses.
- **Broadcast SSID**: Use this toggle button to enable or disable the visibility of the SSID to all the wireless clients within range.

Step 7 Complete the **Security Settings** setup:

a) For **L2 Security**, choose the encryption and authentication type for the network. The sites, buildings, and floors inherit settings from the Global hierarchy. You can override the level of security at the site, building, or floor level.

- **Enterprise**: You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes. By default, the **WPA3** check box is checked.

  To enable AP beacon protection, check the **AP Beacon Protection** check box.

Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP).

WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks. WPA3 is supported on Cisco AireOS Wireless Controllers running Release 8.10 and later, and Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 16.12 and later.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional).

WPA2 isn't supported for the 6-GHz band. For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running versions between Cisco IOS XE Release 17.7 and Cisco IOS XE Release 17.11. For devices running Cisco IOS XE 17.12 or later, you can enable all the radio bands on the same SSID with WPA3 enabled.

- **Personal**: You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes. By default, the **WPA3** check box is checked. If you choose **Personal**, in the **Pass Phrase** field, enter the passphrase key. This key is used as the pairwise master key (PMK) between the clients and authentication server.

  To enable AP beacon protection, check the **AP Beacon Protection** check box.

Note WPA3-Personal brings better protection to individual users by providing a more robust password-based authentication. This authentication makes the brute-force dictionary attack more difficult and time-consuming.

For WPA2-Personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For more information, see Configure site-level overrides for an SSID for enterprise networks, on page 360.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS XE Release 17.7 and later. WPA2 isn't supported for the 6-GHz band.

(Optional) For WPA2-Personal, to configure multi-preshared key (MPSK) support:

1. Click **Configure MPSK**.
2. In the **Configure MPSK** dialog box, click **Add** to add an MPSK.

   You can add up to five MPSKs.

3. From the **Priority** drop-down list, choose a priority.



Note If the priority 0 key isn't configured in the central web authentication (CWA) Flex mode, client connection to the WLAN may fail.

4. From the **Passphrase Type** drop-down list, choose a passphrase type.
5. In the **Passphrase** field, enter a passphrase.
6. Click **Save**.

MPSK isn't supported on Cisco AireOS Wireless Controllers. MPSK applies to Layer 2 security configuration for WPA2-Personal.

- **Open Secured**: From the **Select existing Open SSID** drop-down list, choose an open SSID to redirect the clients to an open-secured SSID. The open-secured policy provides the least security.



Note Fast Transition isn't applicable for open-secured SSID.

Because an open-secured SSID depends on an open SSID, you must have enabled anchor on an open SSID before enabling it on an open-secured SSID.

- **Open**: The open policy provides no security. It allows any device to connect to the wireless network without authentication.



Note If you chose only the **6GHz** radio policy in the **Basic Settings** window, the **Open** option is dimmed.

b) For **Fast Transition (802.11r)**:

- Choose a mode: **Adaptive**, **Enable**, or **Disable**.



Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP. We recommend that you disable fast transition for WLANs using open authentication. Cisco AireOS Wireless Controllers don't support the **Adaptive** fast transition mode.

- Check the **Over the DS** check box to enable fast transitions over a distributed system. By default, fast transition over a distributed system is disabled.

c) Under **WPA2 Encryption**, **WPA3 Encryption** or **WPA2/WPA3 Encryption**, from the available options, choose the required options.

The options available under this section vary based on the settings that you choose under **L2 Security**. These options may be available: **AES(CCMP128)**, **GCMP128**, **CCMP256**, and **GCMP256**

Note This section isn't available for the **Open** security under **L2 Security**.

d) Under **Auth Key Management**, check the check box next to the required options.

Note This section isn't available for the **Open** security under **L2 Security**.

The options available under this section vary based on the fast transition settings. These options may be available:

- For **AES(CCMP128)**: **OWE**, **802.1x (802.1X-SHA1)**, **FT + 802.1x**, **CCKM**, **802.1x-SHA256 (802.1X-SHA2)**, **PSK**, **FT + PSK**, **Easy-PSK**, **PSK-SHA256 (PSK-SHA2)**, **SAE**, **SAE-EXT-KEY**, **FT + SAE**, **FT + SAE-EXT-KEY**
- For **GCMP128**: **SUITEB-1X**
- For **CCMP256**: **SUITEB192-1X**
- For **GCMP256**: **FT + 802.1x**, **802.1x-SHA256 (802.1X-SHA2)**, **SUITEB192-1X**
- **Timestamp Tolerance (in milliseconds)** (for CCKM): Enter the CCKM tolerance level in milliseconds. The valid range is from 1000 through 5000. The default value is 1000. Authenticated client devices can roam from one AP to another AP without any perceptible delay during reassociation. CCKM tolerance level isn't applicable for Cisco AireOS Wireless Controllers.

e) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the enterprise wireless network SSID.

For more information, see Configure AAA server for an enterprise wireless network, on page 364.

Check one or more of the available check boxes:

- To enable the AAA override functionality, check the **AAA Override** check box.

  By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.
- **Identity PSK** (for Personal Layer 2 security): Check this check box to enable the creation of unique preshared keys for individuals or groups of users in the SSID. If you check this check box, the **Enable Posture** check box is displayed.
- **MAC Filtering** (for Enterprise Layer 2 security): Check this check box to enable MAC-based access control or security on the wireless network.

Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients**: Check this check box to deny clients with randomized MAC addresses. This option is supported for Cisco AireOS Wireless Controllers running Release 8.10 MR5 and later, and Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.5 and later.
- **Enable Posture**: Check this check box to enable posture assessment. If you enable MAC filtering, this check box is dimmed.

  Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients' access to protected areas of a network.

  From the **Pre-Auth IPv4 ACL List Name** and **Pre-Auth IPv6 ACL List Name** drop-down lists, choose the ACL list names for the required IP address type. If the **URL ACL Name** drop-down list is displayed, optionally choose a URL ACL name.



Note AAA configuration is mandatory for posturing. Click **Configure AAA** to add AAA servers for the enterprise wireless network SSID.

f) Click **Next**.

Step 8 Complete the **Advance Settings** setup:

a) For **MFP Client Protection**, choose **Optional**, **Required**, or **Disabled**.



Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and the client is also configured for WPA2 and supports CCXv5 MFP).

MFP client protection is supported only on Cisco AireOS Wireless Controllers. MFP client protection isn’t supported for the 6-GHz band.

b) For **Protected Management Frame (802.11w)**, choose the required option.



Note The options available under **Protected Management Frame (802.11w)** vary based on the settings that you choose under **L2 Security**. These options may be available: **Optional**, **Required**, or **Disabled**

c) To configure all the 11k-capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming, use the **11k - Neighbor List** toggle button.

To facilitate roaming, a 11k-capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for the next roam from the response frame.

d) To enable or disable RADIUS profiling on a WLAN, use the **Radius Client Profiling** toggle button.

Note At least one AAA or PSN server is required to enable this feature.

e) To enable or disable the coverage hole detection functionality, use the **Coverage Hole Detection** toggle button.

f) Under **WLAN Timeouts**, do these tasks:

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization. In the corresponding field, enter the session timeout in seconds. The valid range is from 1 through 86400.

  Note By default, **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer. In the corresponding field, enter the client exclusion time in seconds. The valid range is from 0 through 2147483647.

  Note When a user fails to authenticate, the wireless controller denies the client connection. The client isn't allowed to connect to the network until the exclusion timer expires. By default, **Client Exclusion** is enabled with a timeout of 180 seconds.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout for a WLAN. In the corresponding field, enter the user idle timeout in seconds. The valid range is from 15 through 100000.

  If the data sent by the client is more than the threshold specified by the user idle timeout, the client is considered to be active, and the wireless controller begins another timeout period.

  Note By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

g) Under **11v BSS Transition Support**, do these tasks:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

  Note The BSS Max idle period is the time frame during which an AP doesn't disassociate a client because of nonreceipt of frames from the connected client.

- **Directed Multicast Service**: Check this check box to enable directed multicast service.

Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer period and saves the battery power.

h) (Optional) For **NAS-ID**:

1. From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID).

   To specify a custom script for the NAS ID, from the **NAS-ID Opt** drop-down list, choose **Custom Option** and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Catalyst Center doesn't support the special characters ? " < and trailing spaces for the custom script.

   Note Catalyst Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later.

2. (Optional) Click **+** to add another NAS ID. You can add up to three NAS IDs.

   Note Catalyst Center applies only one NAS ID for Cisco AireOS Wireless Controllers. You can overwrite the NAS ID at the site-level from the **Design** > **Network Settings** > **Wireless** window.

i) (Optional) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100000000000. The value must be a multiple of 500.

Note This configuration is applicable for Cisco AireOS Wireless Controllers. To configure the client rate limit for Cisco AireOS Wireless Controllers, click the menu icon and choose **Design** > **Feature Templates** > **Wireless** > **Advanced SSID Configuration**. For more information, see Create a feature template for advanced SSID, on page 512.

The valid ranges for client rate limit on Cisco IOS XE devices include:

- The valid range for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67000000000 bits per second.
- The valid range for Cisco Catalyst 9800-CL Wireless Controllers is from 8000 through 10000000000 bits per second.
- The valid range for Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2000000000 bits per second.
- The valid range for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100000000000 bits per second.

j) Click **Next**.

Step 9 (Optional) Complete the **Associate Feature Templates to SSID** setup:

a) Check the check box next to the required feature template.

If you want to create a feature template, click **Add** and configure the required settings. For more information, see Create a feature template for advanced SSID, on page 512.

b) Click **Next**.

Step 10 Complete the **Associate SSID to Wireless Network Profile** setup to associate at least one wireless network profile with the SSID:

If you want to...	Then...
create a network profile and associate it with the SSID	**a.** Click **Add Profile**. **b.** In the **Add Profile** dialog box, configure the profile settings. For more information, refer to Create network profiles for wireless, on page 460. **c.** Click **Associate Profile**.
associate an existing network profile	**a.** Click **Edit** for the required network profile. **b.** In the **Edit** dialog box, update the profile settings if necessary. For more information, refer to Create network profiles for wireless, on page 460. **c.** Click **Associate Profile**.
disassociate an associated network profile	**a.** Click **Edit** for the required network profile. **b.** In the **Edit** dialog box, click **Disassociate Profile**.
search for a network profile	in the **Search Network Profile** field, enter a value.
filter the network profiles based on the association status with SSID	from the **Associated** drop-down list, choose the required option.

Step 11 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 12 Click **Save**.

The SSID is created.

Configure site-level overrides for an SSID for enterprise networks

You can create SSIDs at the Global hierarchy. The areas, buildings, and floors inherit settings from the Global hierarchy. You can override these settings at the area, building, or floor level:

- **WLAN Profile Name**
- **Policy Profile Name**

- **Radio Policy**
- **L2 Security**
- **Fast Transition (802.11r)**
- **WPA2 Encryption**, **WPA3 Encryption**, or **WPA2/WPA3 Encryption**
- **Auth Key Management**
- **Authentication, Authorization, and Accounting Configuration**
- **Protected Management Frame (802.11w)**
- **Radius Client Profiling**
- **NAS-ID**
- **Configure Client Rate Limit**
- **MAC Filtering**
- **MPSK**
- **AAA Override**
- **AP Beacon Protection**

If you override a setting at the building level, the subsequent floor inherits the new setting. This procedure describes how to configure site-level overrides for an SSID for enterprise networks.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Wireless**.

Step 2 From the left hierarchy tree, choose the site, building, or floor for which you want to configure the overrides.

Hover your cursor over the inherit icon next to the SSID to view the origin of this setting.

Step 3 Check the check box next to the SSID, and click **Edit**.

Step 4 In the **Basic Settings** window, edit the required settings.

Note

- While configuring site-level overrides for the SSID, we recommend that you enter a unique name for the WLAN profile across the sites that are managed by the same wireless controller. Provisioning a wireless controller with the SSID overridden at different sites but with the same WLAN profile name or policy profile name results in provisioning failure.
- If an SSID associated with a network profile has site-level overrides, Catalyst Center uses the WLAN profile name or policy profile name from the overridden SSID during wireless controller provisioning for the corresponding sites. This rule applies when the overridden site is associated with the wireless controller's network profiles and is managed by the same wireless controller.

Step 5 (Optional) In the **Security Settings** window, edit the required settings.

For more information, see Create SSIDs for an enterprise wireless network, on page 351.

Step 6 (Optional) In the **Advanced Settings** window, edit the required settings.

For more information, see Create SSIDs for an enterprise wireless network, on page 351.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Click **Save**.
Site-level overrides are configured for the SSID.

Create Preauthentication Access Control Lists

Using the Preauthentication ACL feature, you can create a preauthentication ACL for web authentication to allow certain types of traffic before authentication is complete. This ACL is referenced in the access-accept of Cisco Identity Services Engine (ISE) and defines the traffic that is permitted and the traffic that is denied by the ACL. After the ACLs are configured on the Cisco Wireless Controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU. You can configure both IPv4 and IPv6 ACLs.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Security Settings**.

Step 5 Click the **Pre-Auth ACLs** tab.

Step 6 Under the **Pre-Auth Access Control Lists** area, click **Add** to create a preauthentication ACL.

Step 7 In the **New Pre-Auth ACL** slide-in pane, do these steps:

a. In the **Pre-Auth ACL List Name** field, enter a name for the ACL list to be used on Catalyst Center.

b. In the **Pre-Auth ACL Name** field, enter a name for the ACL to be configured on wireless controller.

Step 8 Click the **IP Addresses** tab and do these steps:

a. Choose the ACL type that you're creating: **IPV4** or **IPV6**.

b. Use the **Include auto rules generated by Catalyst Center** toggle button to enable or disable pushing the Catalyst Center-generated rules to the applicable SSIDs.

By default, this toggle button is enabled. When enabled, Catalyst Center pushes the autogenerated rules to the applicable SSIDs. Autogenerated rules allow DHCP, DNS, AAA, and other applicable ports and IP addresses that are created as part of the default preauthentication rule. The default rules are created based on the IP addresses configured in the network settings.

For fabric SSIDs, if the DHCP or DNS IP address in the IP Address Manager differs from the IP address in the network settings, additional rules are created to allow these IP addresses.



Note If you disable this toggle button, you must ensure that the custom preauthentication ACL rule includes all the DHCP, DNS, and AAA servers that are mapped to WLANs.

c. From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL.

d. In the **Source Port** field, enter the source port number.

The valid range is from 0 to 65535. You can enter either a single port number (for example, 120) or a range of port numbers (for example, 0-65535).

The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.



Note If the selected protocol does not require or support port configuration (such as PIM), this field is dimmed.

e. In the **Source IP Address** field, enter the IP address based on the IP address type.

If the IP address type is...	Then...
IPv4	From the **Source Subnet** drop-down list, choose a value for the source subnet.
IPv6	From the **Prefix Length** drop-down list, choose a prefix length.

f. In the **Destination Port** field, enter the destination port number.

The valid range is from 0 to 65535. You can enter either a single port number (for example, 120) or a range of port numbers (for example, 0-65535).



Note If the selected protocol does not require or support port configuration (such as PIM), this field is dimmed.

g. In the **Destination IP Address** field, enter the IP address based on the IP address type.

If the IP address type is...	Then...
IPv4	From the **Destination Subnet** drop-down list, choose a value for the destination subnet.
IPv6	From the **Prefix Length** drop-down list, choose a prefix length.

h. To add multiple rules, click the plus icon. You can add up to 256 rules.



Note For Cisco AireOS Wireless Controller, you can configure up to 64 rules.

Step 9 Click the **Walled Garden URLs** tab to add specific URLs to the allowed list for the web authentication of captive portal and walled garden.

Authentication isn't required to access the allowed list of URLs. When you try to access sites that aren't in the allowed list, you're redirected to the login window.

a. In the **URL** field, enter the URL and click the plus icon to add the URL to the allowed list for web authentication. You can add up to 16 URL entries.

- For Cisco AireOS Wireless Controller: A valid URL must have at least one period (.). Other special characters aren't supported. For example, cisco.com and www.cisco.com.
- For Cisco Catalyst 9800 Series Wireless Controller: A valid URL must have at least one period (.). The special characters . * - _ are supported. For example, www.cisco.com, *.cisco.com, and www.cisco-.com.

Step 10 Click **Save**.

What to do next

Map the ACL with the SSID while creating SSIDs. For more information, refer to Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

Configure AAA server for an enterprise wireless network

Before you begin

- Make sure you have defined the AAA server under **System Settings** > **External Services** > **Authentication and Policy Servers**.

Note In dual-stack deployments, make sure that the AAA server IP address type for the SSID matches the wireless controller IP address type. If a wireless controller is discovered or added to the inventory using an IPv4 address, configure IPv4 AAA servers for the SSID. If a wireless controller is discovered or added to the inventory using an IPv6 address, configure IPv6 AAA servers for the SSID.

- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions, and the appropriate RBAC scope to perform this procedure.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **SSIDs**.

Step 5 From the **SSID** table, in the **AAA Servers** column, click **Configure AAA** for the SSID for which you want to configure the AAA server.

Step 6 From the **Configure Authentication and Authorization Server** drop-down list of the **Configure AAA Server** slide-in pane, you can either search for a server IP address by entering its name in the **Search** field or choose the AAA IP address.

Note
- The **Configure AAA** option is not supported for the Mobility Express (ME) devices.
- You must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Catalyst Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Step 7 Click + to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of enterprise wireless network.

Step 8 From the **Additional Server** drop-down list, choose the server IP address.

Step 9 To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box.

Note You must configure an accounting server for an SSID to push the accounting configuration for the SSID.

Step 10 To configure a different accounting server for an SSID:

a) From the **Configure Accounting Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose the accounting server IP address.

b) Click + to add an **Additional Server**.

Note You can configure a maximum of six accounting servers for an SSID of enterprise wireless network.

c) From the **Additional Server** drop-down list, choose the server IP address.

Step 11 Click **Configure**.

Note Catalyst Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Catalyst Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Catalyst Center creates the new WLAN profiles equal to the number of floors.

You must reprovision the device to override the AAA servers at the site level. See Wireless device provisioning overview, on page 617.

Create SSIDs for a guest wireless network

This procedure explains how to create SSIDs for a guest wireless network.

A user with role-based access control (RBAC) with write permission for **Network Design** > **Profiles and Settings** can create and modify wireless design artifacts. This includes SSIDs, Guest Portals, and Guest Policies. For more information, refer to "Catalyst Center user role and permissions" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **SSIDs**.

Step 5 In the **SSID** table, hover your cursor over **Add**, and choose **Guest**.

Step 6 In the **Wireless SSID** workflow, complete the **Basic Settings** setup:

a) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.

b) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

c) (Optional) In the **Policy Profile Name** field, change the policy profile name.

By default, Catalyst Center automatically copies the WLAN profile name as the policy profile name.

d) (Optional) Use the **Copy to Policy Profile Name** check box for one of these options:

- Automatically copy the WLAN profile name as the policy profile name.
- Enter a different name for the policy profile.

e) In the **Radio Policy** area, do these tasks:

- Check the **2.4GHz** check box to create the WLAN for 2.4-GHz.
- Check the **5GHz** check box to create the WLAN for 5-GHz.
- Check the **6GHz** check box to create the WLAN for 6-GHz. This band is supported for devices running Cisco IOS XE Release 17.7 or later.

- From the **802.11b/g Policy** drop-down list, choose a policy.

Note This drop-down list is available only when you check the **2.4GHz** check box.

- Check the **Band Select** check box to choose the required band.

Note This check box is available only when you check both the **2.4GHz** and **5GHz** check boxes.

- Check the **6 GHz Client Steering** check box to enable client steering.

Note This check box is available only when you check the **6GHz** check box.

f) To enable or disable the fastlane capabilities on the network, use the **Fast Lane** toggle button.

By enabling fastlane, you can configure the iOS devices to receive an optimized level of wireless connectivity and enhanced QoS.

When fastlane capabilities are enabled, QoS selection isn't applicable.

g) In the **Quality of Service(QoS)** area, do these tasks:

- From the **Egress** drop-down list, choose an egress QoS: **VoIP (Platinum)**, **Video (Gold)**, **Best Effort (Silver)**, or **Non-real Time (Bronze)**
- From the **Ingress** drop-down list, choose an ingress QoS: **VoIP (Platinum)**, **Video (Gold)**, **Best Effort (Silver)**, or **Non-real Time (Bronze)**

Note Ingress QoS is applicable only for Cisco IOS XE wireless controllers.

The QoS selection isn't applicable when **Fast Lane** is enabled. For Cisco IOS XE wireless controllers, QoS (both egress and ingress) is set to empty. For Cisco AireOS Wireless Controllers, the egress QoS is set to **VoIP (Platinum)**.

h) Under **SSID STATE**, use the toggle buttons to enable or disable these settings:

- **Admin Status**: Use this toggle button to turn on or turn off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and are accessible, and the APs still require licenses.
- **Broadcast SSID**: Use this toggle button to enable or disable the visibility of the SSID to all the wireless clients within range.

Step 7 Complete the **Security Settings** setup:

a) For the **L2 SECURITY** area, choose the L2 encryption and authentication type:

- **Enterprise**: You can configure either the **WPA2** or the **WPA3** security authentication type by checking the respective check boxes. By default, the **WPA2** check box is enabled.

  To enable AP beacon protection, check the **AP Beacon Protection** check box.

  Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Fast transition is applicable for enterprise WPA2 SSID.

  WPA3 security authentication is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

  For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional).

  WPA2 isn't supported for the 6-GHz band. For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running versions between Cisco IOS XE Release 17.7 and Cisco IOS XE Release 17.11. For devices running Cisco IOS XE 17.12 or later, you can enable all the radio bands on the same SSID with WPA3 enabled.

- **Personal**: You can configure both **WPA2** and **WPA3** or configure **WPA2** and **WPA3** individually by checking the respective check boxes.

  To enable AP beacon protection, check the **AP Beacon Protection** check box.

  Note WPA3-Personal security authentication brings better protection to individual users by providing more robust password-based authentication. This makes the brute-force dictionary attack more difficult and time-consuming.

  Enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between the clients and the authentication server.

  For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS XE Release 17.7 and later. WPA2 isn't supported for the 6-GHz band.

  (Optional) For WPA2-Personal, to configure multi-preshared key (MPSK) support:

  1. Click **Configure MPSK**.
  2. In the **Configure MPSK** dialog box, click **Add** to add an MPSK.

     You can add up to five MPSKs.
  3. From the **Priority** drop-down list, choose a priority.



Note If the priority 0 key isn't configured in central web authentication (CWA) Flex mode, client connection to the WLAN may fail.

4. From the **Passphrase Type** drop-down list, choose a passphrase type.
5. In the **Passphrase** field, enter a passphrase.
6. Click **Save**.

MPSK isn't supported on Cisco AireOS Wireless Controllers. MPSK applies to the Layer 2 security configuration for WPA2-Personal.

- **Open Secured**: From the **Select existing Open SSID** drop-down list, choose an open SSID to associate with the open SSID. Associating secures the open SSID. You must have an open SSID created before associating it with the open secured SSID.



Note Fast Transition isn't applicable for open-secured SSID.

Because open-secured SSID depends on open SSID, you must have enabled the anchor on open SSID before enabling it on open-secured SSID.

- **Open**: The open policy provides no security. It allows any device to connect to the wireless network without authentication.



Note If you chose only the **6GHz** radio policy in the **Basic Settings** window, the **Open** option is dimmed.

b) For **Fast Transition (802.11r)**:

- Choose a mode: **Adaptive**, **Enable**, or **Disable**.



Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP. We recommend that you disable fast transition for WLANs using open authentication. Cisco AireOS Wireless Controllers don't support the **Adaptive** fast transition mode.

- Check the **Over the DS** check box to enable fast transitions over a distributed system. By default, fast transition over a distributed system is disabled.

c) Under **WPA2 Encryption**, **WPA3 Encryption**, or **WPA2/WPA3 Encryption**, from the available options, choose the required options.

The options available under this section vary based on the settings that you chose under **L2 Security**. These options may be available: **AES(CCMP128)**, **GCMP128**, **CCMP256**, **GCMP256**

Note This section isn't available for the **Open** security under **L2 Security**.

d) Under **Auth Key Management**, check the check box next to the required options.

Note This section isn't available for the **Open** security under **Level of Security**. These options may be available:

- For **AES(CCMP128)**: **OWE**, **802.1x (802.1X-SHA1)**, **FT + 802.1x**, **CCKM**, **802.1x-SHA256 (802.1X-SHA2)**, **PSK**, **FT + PSK**, **Easy-PSK**, **PSK-SHA256 (PSK-SHA2)**, **SAE**, **SAE-EXT-KEY**, **FT + SAE**, **FT + SAE-EXT-KEY**
- For **GCMP128**: **SUITEB-1X**
- For **CCMP256**: **SUITEB192-1X**
- For **GCMP256**: **FT + 802.1x**, **802.1x-SHA256 (802.1X-SHA2)**, **SUITEB192-1X**

The options available under this section vary based on the fast transition settings.

- **Timestamp Tolerance (in milliseconds)** (for CCKM): Enter the CCKM tolerance level in milliseconds. The valid range is from 1000 through 5000. The default value is 1000. Authenticated client devices can roam from one AP to another AP without any perceptible delay during reassociation. CCKM tolerance level isn't applicable for Cisco AireOS Wireless Controllers.

e) For the **L3 Security** setting, choose the L3 encryption and authentication type:

- **Web Policy**: Provides a higher level of L3 security.

  For **Authentication Server**, configure these authentication server settings:

Authentication server type	Description
Central Web Authentication	Use AAA server for central web authentication (CWA). (Optional) If you choose Cisco ISE for CWA, from the **What kind of portal are you creating today?** drop-down list, choose the type of portal you want to create: • **Self Registered**: The guests are redirected to the self-registered guest portal to register by providing information to automatically create an account. • **HotSpot**: The guests can access the network without providing any credentials. (Optional) If you choose Cisco ISE for CWA, from the **Where will your guests redirect after successful authentication?** drop-down list, choose where you want to redirect the guests after successful authentication: • **Success Page**: The guests are redirected to the **Authentication Success** window. • **Original URL**: The guests are redirected to the URL that they had originally requested. • **Custom URL**: The guests are redirected to the custom URL that is specified here. Enter a redirect URL in the **Redirect URL** field.
• **Web Authentication Internal** • **Web Authentication External**	Web authentication or Web Auth is a Layer 3 security method that allows a client to pass Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) traffic only until they have passed some form of authentication. For web authentication internal, the client is redirected to a window that is constructed by the Cisco Wireless Controller. For web authentication external, the client is redirected to the specified URL. Enter a redirect URL in the **Web Auth Url** field.
• **Web Passthrough Internal** • **Web Passthrough External**	Web passthrough is used for guest access and doesn't requires authentication credentials. In web passthrough authentication, wireless users are redirected to the Usage Policy window when they use the internet for the first time. After accepting the policy, users are allowed to use the internet.

• **Open**: There is no security at the Layer 3 level and any device can connect to the SSID.

f) If you choose **Web Authentication Internal**, **Web Authentication External**, **Web Passthrough Internal**, or **Web Passthrough External**, in the **Timeout Settings for sleeping clients** area, choose an authentication setting for sleeping clients:

• **Always authenticate**: Enables authentication for sleeping clients.

- **Authenticate after**: Enter how many minutes you want sleeping clients to be remembered for before reauthentication becomes necessary. The valid range is from 10 minutes through 43200 minutes, and the default duration is 720 minutes.



Note Clients with guest access and web authentication are allowed to sleep and wake up without having to reauthenticate through the login window. You can configure how long a client is remembered on a WLAN and a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is less than the time configured on the sleeping timer of the WLAN, the lifetime of the client is used as the sleeping time.

g) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the guest wireless network SSID.

For more information, see Configure AAA server for a guest wireless network, on page 378.

(Optional) Complete these configurations:

- To enable the AAA override functionality, check the **AAA Override** check box.

  By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

- **Identity PSK** (for Personal Layer 2 security): Check this check box to enable the creation of unique preshared keys for individuals or groups of users in the SSID.

- **MAC Filtering** (for Enterprise Layer 2 security): Check this check box to enable MAC-based access control or security in the wireless network.



Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients**: Check this check box to deny clients with randomized MAC addresses. This option is supported for Cisco AireOS Wireless Controllers running Release 8.10 MR5 and later, and Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.5 and later.

- **Pre-Auth IPv4 ACL List Name** and **Pre-Auth IPv6 ACL List Name**: Choose the ACL list names for the required IP address type.

  If the **URL ACL Name** drop-down list is displayed, optionally choose a URL ACL name.

  These drop-down lists are available only when you choose **Central Web Authentication** and **Web Authentication External**.



Note You must add the authorization profile for URL filter manually on Cisco ISE for Cisco IOS XE devices. When you select both IPv4 and IPv6 preauthentication ACLs, the authorization profile on Cisco ISE uses the IPv6 ACL by default.

h) Click **Next**.

Step 8 Complete the **Advance Settings** setup:

a) For **MFP Client Protection**, choose **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and the client is also configured for WPA2 and supports CCXv5 MFP).

MFP client protection is supported only on Cisco AireOS Wireless Controllers. MFP client protection isn't supported for the 6-GHz band.

b) For **Protected Management Frame (802.11w)**, choose the required option.

Note The options available under **Protected Management Frame (802.11w)** vary based on the settings that you chose under **Level of Security**. These options may be available: **Optional**, **Required**, or **Disabled**

c) To configure all the 11k-capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming, use the **11k - Neighbor List** toggle button.

Note To facilitate roaming, a 11k-capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for the next roam from the response frame.

d) To enable or disable RADIUS profiling on a WLAN, use the **Radius Client Profiling** toggle button.

Note At least one AAA or PSN server is required to enable this feature.

e) To enable or disable the coverage hole detection functionality, use the **Coverage Hole Detection** toggle button.

f) Under **WLAN Timeouts**, do these tasks:

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization. In the corresponding field, enter the session timeout in seconds. The valid range is from 1 through 86400.

Note By default, **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer. In the corresponding field, enter the client exclusion time in seconds. The valid range is from 0 through 2147483647.

  Note When a user fails to authenticate, the wireless controller denies the client connection. The client isn't allowed to connect to the network until the exclusion timer expires. By default, **Client Exclusion** is enabled with a timeout of 180 seconds.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout period for a WLAN. In the corresponding field, enter the user idle timeout in seconds. The valid range is from 15 through 100000.

  Note If the data sent by the client is more than the threshold quota specified as the user idle timeout period, the client is considered to be active and the wireless controller refreshes for another timeout period.

  By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

g) For **11v BSS Transition Support**:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value isn't transmitted using the association and reassociation response frame from the APs to the client.

  Note The BSS Max idle period is the time frame during which an AP doesn't disassociate a client because of nonreceipt of frames from the connected client.

- **Directed Multicast Service**: Check this check box to enable directed multicast service.

  Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer period and saves the battery power.

h) (Optional) For **NAS-ID**:

1. From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID).

   (Optional) To specify a custom script for the NAS ID, choose **Custom Option** from the **NAS-ID Opt** drop-down list and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Catalyst Center doesn't support the special characters ? " < and trailing spaces for the custom script.

Note Catalyst Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later.

2. (Optional) Click + to add another network access server identifier. You can add up to three NAS IDs.

Note Catalyst Center applies only one NAS ID for Cisco AireOS Wireless Controllers. You can overwrite the NAS ID at the site-level from the **Design** > **Network Settings** > **Wireless** window.

i) (Optional) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100000000000. The value must be a multiple of 500.

Note This configuration is applicable for Cisco AireOS Wireless Controllers. To configure the client rate limit for Cisco AireOS Wireless Controllers, click the menu icon and choose **Design** > **Feature Templates** > **Wireless** > **Advanced SSID Configuration**. For more information, see Create a feature template for advanced SSID, on page 512.

The valid ranges for client rate limit on Cisco IOS XE devices include:

- The valid range for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67000000000 bits per second.
- The valid range for Cisco Catalyst 9800-CL Wireless Controller is from 8000 through 10000000000 bits per second.
- The valid range for Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2000000000 bits per second.
- The valid range for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100000000000 bits per second.

j) Click **Next**.

Step 9 (Optional) Complete the **Associate Feature Templates to SSID** setup:

a) Check the check box next to the required feature template.

If you want to create a feature template, click **Add** and configure the required settings. For more information, see Create a feature template for advanced SSID, on page 512.

b) Click **Next**.

Step 10 Complete the **Associate SSID to Wireless Network Profile** setup to associate at least one wireless network profile with the SSID:

If you want to...	Then...
create a network profile and associate it with the SSID	**a.** Click **Add Profile**. **b.** In the **Add Profile** dialog box, configure the profile settings. For more information, refer to Create network profiles for wireless, on page 460. **c.** Click **Associate Profile**.
associate an existing network profile	**a.** Click **Edit** for the required network profile. **b.** In the **Edit** dialog box, update the profile settings if necessary. For more information, refer to Create network profiles for wireless, on page 460. **c.** Click **Associate Profile**.
disassociate an associated network profile	**a.** Click **Edit** for the required network profile. **b.** In the **Edit** dialog box, click **Disassociate Profile**.
search for a network profile	in the **Search Network Profile** field, enter a value.
filter the network profiles based on the association status with SSID	from the **Associated** drop-down list, choose the required option.

Step 11 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 12 Click **Save**.

The SSID is created.

Configure site-level overrides for an SSID for guest networks

You can create SSIDs at the Global hierarchy. The areas, buildings, and floors inherit settings from the Global hierarchy. You can override these settings at the area, building, or floor level:

- **WLAN Profile Name**
- **Policy Profile Name**
- **Radio Policy**
- **L2 Security**
- **Fast Transition (802.11r)**
- **WPA2 Encryption**, **WPA3 Encryption**, or **WPA2/WPA3 Encryption**
- **Auth Key Management**
- **Authentication, Authorization, and Accounting Configuration**

- **Protected Management Frame (802.11w)**
- **Radius Client Profiling**
- **NAS-ID**
- **Configure Client Rate Limit**
- **MAC Filtering**
- **MPSK**
- **AAA Override**
- **AP Beacon Protection**

If you override a setting at the building level, the subsequent floor inherits the new setting. This procedure describes how to configure site-level overrides for an SSID for guest networks.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Wireless**.

Step 2 From the left hierarchy tree, choose the site, building, or floor for which you want to configure the overrides.

Hover your cursor over the inherit icon next to the SSID to view the origin of this setting.

Step 3 Check the check box next to the SSID, and click **Edit**.

Step 4 In the **Basic Settings** window, edit the required settings.

Note

- While configuring site-level overrides for the SSID, we recommend that you enter a unique name for the WLAN profile across the sites that are managed by the same wireless controller. Provisioning a wireless controller with the SSID overridden at different sites but with the same WLAN profile name or policy profile name results in provisioning failure.
- If an SSID associated with a network profile has site-level overrides, Catalyst Center uses the WLAN profile name or policy profile name from the overridden SSID during wireless controller provisioning for the corresponding sites. This rule applies when the overridden site is associated with the wireless controller's network profiles and is managed by the same wireless controller.

Step 5 (Optional) In the **Security Settings** window, edit the required settings.

For more information about editing the settings, see Create SSIDs for a guest wireless network, on page 366.

Step 6 (Optional) In the **Advanced Settings** window, do this task:

For more information about editing the settings, see Create SSIDs for a guest wireless network, on page 366.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Click **Save**.

Site-level overrides are configured for the SSID.

Configure AAA server for a guest wireless network

Before you begin

- Make sure you have defined the AAA server under the **System Settings** > **External Services** > **Authentication and Policy Servers** window.

Note In dual-stack deployments, make sure that the AAA server IP address type for the SSID matches the wireless controller IP address type. If a wireless controller is discovered or added to the inventory using an IPv4 address, configure IPv4 AAA servers for the SSID. If a wireless controller is discovered or added to the inventory using an IPv6 address, configure IPv6 AAA servers for the SSID.

- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **SSIDs**.

Step 5 From the **SSID** table, in the **AAA Servers** column, click **Configure AAA** for the SSID for which you want to configure the AAA server.

Step 6 From the **Server** drop-down list of the **Configure AAA Server** slide-in pane, you can either search for a AAA IP address by entering its name in the **Search** field or choose AAA IP address.

Note

- You must configure at least one AAA or Policy Service Node (PSN) server for Central Web Authentication (CWA) SSIDs of guest wireless network.
- Catalyst Center-generated preauthentication ACLs are created only for the configured AAA or PSN servers for CWA SSIDs of guest wireless networks. If you upgrade from an earlier release, to ensure that there is no compliance mismatch, you must reprovision the wireless controller.
- Catalyst Center allows you to map AAA server in any combination of identity services engine PSNs and third-party AAA IPs.
- In the **Server** drop-down list, the **AAA** IP addresses and the PSN IP addresses are grouped in the corresponding sections.
- The **Configure AAA** option is not supported for Mobility Express (ME) devices.
- You must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Catalyst Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Step 7 Click + to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 8 From the **Additional Server** drop-down list, choose the server IP address.

Step 9 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 10 To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box.

Note You must configure an accounting server for an SSID to push the accounting configuration for the SSID.

Step 11 To configure a different accounting server for an SSID:

a) From the **Configure Accounting Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose the accounting server IP address.

b) Click + to add an **Additional Server**.

Note You can configure a maximum of six accounting servers for an SSID of enterprise wireless network.

c) From the **Additional Server** drop-down list, choose the server IP address.

Step 12 Click **Configure**.

Note Catalyst Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Catalyst Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Catalyst Center creates the new WLAN profiles equal to the number of floors.

You must reprovision the device to override the AAA servers at the site level. See Wireless device provisioning overview, on page 617.

Create SSID scheduler

You can create an SSID scheduler to enable or disable WLAN based on time zone.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **SSIDs**.

Step 5 In the **SSID** table, click **SSID Scheduler**.

Step 6 In the **SSID Scheduler** window, click **Add**.

Step 7 In the **Create Scheduler** slide-in pane, do these steps:

a) Enter a unique name for the SSID scheduler that you want to create.
b) Click the **Client Deny** radio button for denying clients from joining SSID.
c) Click the **Enable SSID** radio button to schedule SSID broadcasting.
d) Choose the **Scheduler Type Daily**, **Weekly**, or **Monthly** and complete the required settings.
e) From the **Time Zone** drop-down list, choose the time zone.
f) Click **Save**.

The created SSID scheduler appears in the **SSID Scheduler** table.

Step 8 To edit the SSID scheduler:

a) From the **SSID Scheduler** table, choose the SSID scheduler and click **Edit**.
b) In the **Edit SSID Scheduler** slide-in pane, make the required changes and click **Save.**

Step 9 To delete the SSID scheduler, choose the SSID scheduler and click **Delete.**

Step 10 To view the details of the SSID scheduler, choose the SSID scheduler and click **Scheduler History**.

Note To view the **Scheduler History**, you must install the Assurance package.

What to do next

Enable the SSID scheduler for wireless controller. For more details, see Add SSIDs to a network profile, on page 460.

Create a wireless interface

You can create wireless interfaces only in nonfabric deployments.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Interfaces & VLAN Groups**.

Step 5 Click the **Interfaces** tab.

Step 6 From the **Wireless Interfaces** table, click **Add**.

Step 7 Configure the wireless interface settings in the **Create a Wireless Interface** slide-in pane:

a) In the **Interface Name** field, enter the dynamic interface name.

b) In the **VLAN ID** field, enter the VLAN ID for the interface.

For Cisco AireOS Wireless Controllers, the valid range is from 1 through 4094. For Cisco Catalyst 9800 Series Wireless Controllers, the valid range is from 2 through 4094.

Step 8 Click **Save**.

The wireless interface is created and displayed in the **Wireless Interfaces** table.

Design and provision VLAN groups for nonfabric deployments

Catalyst Center allows you to configure networks with multiple broadcast domains through different VLANs. When the same set of APs broadcast the same WLAN, the broadcast domains are controlled through multiple VLANs on the same WLAN through interface groups.

Catalyst Center interface groups are logical groups of interfaces that facilitate user configuration, where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface can be part of multiple interface groups. A WLAN can be associated with an interface or interface group.

Note The interface group name and the interface name can’t be the same.

The Catalyst Center VLAN group feature maps a WLAN to a single VLAN or multiple VLANs using VLAN groups. VLAN groups can be associated to policy profiles.

This procedure explains how to design and provision the interface or VLAN groups for nonfabric deployments.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Interfaces & VLAN Groups**.

Step 5 Click the **VLAN Groups** tab.

Step 6 From the **VLAN Group** table, click **Add**.

Step 7 In the **Add VLAN Group** slide-in pane, do these steps:

a) Enter a valid **VLAN Group Name**

b) Select single or multiple interfaces from the list.

c) Click **Save**.

Note If you select more than 15 interfaces, the selected interfaces might not be displayed correctly onscreen.

Step 8 In the **Edit Network Profile** window, the VLAN group is associated with the SSID.

For information on how to create an SSID, see Create SSIDs for an Enterprise Wireless Network.

Step 9 To add more SSIDs to the VLAN group, click **Add SSID**.

Step 10 Choose **Interface** or **VLAN** group.

Step 11 Click the add icon to create a new interface or VLAN group.

Note Interface or VLAN group isn't applicable for FlexConnect local switching.

Step 12 Click **Save**.

Step 13 In **Configure Interface and VLAN**, you can view the list of interface names, interface group names, and other parameters required to configure the interface and VLAN.

Note An interface group can't contain more than 64 interfaces.

Step 14 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

Step 15 Select the device.

Step 16 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 17 Review the details on the **Assign Site**, **Configuration**, **Feature Templates**, **Advanced Configuration**, and **Summary** windows. On each window, click **Next** to proceed to the next window.

Step 18 Click **Deploy**.

The **Provision Device** dialog box opens.

Step 19 Choose **Now** and click **Apply**.

The message **Task Scheduled view status in Tasks** is displayed.

Create a wireless radio frequency profile

You can either use the default radio frequency profiles (LOW, TYPICAL, HIGH), or create custom radio frequency profiles.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** area, hover your cursor over **Add** and choose **Basic RF Profile**.

Step 3 In the **Profile Name** field of the **Create Wireless Radio Frequency Profile** window, enter the RF profile name.

Step 4 Do this configuration in the **2.4 GHz** tab:

a) Ensure that the **2.4 GHz** toggle button is enabled.

Note

- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **2.4 GHz** toggle button, Catalyst Center disables the Admin status of the **2.4 GHz** RF profile.
- For Cisco AireOS Wireless Controller, if you disable the **2.4 GHz** toggle button and reprovision the wireless controller or AP, Catalyst Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of the corresponding radios on the APs.
- For Cisco AireOS Wireless Controller, when you disable the Admin status for the 2.4-GHz band on the RF profile, Catalyst Center changes the XOR radio on the APs using that RF profile to manual 5-GHz mode. If you enable the Admin status later and reprovision the AP, Catalyst Center changes the radio to automatic mode enabling the usage of 2.4-GHz and 5-GHz bands, and monitor mode. So, if you want to disable the Admin status for the 2.4-GHz band on XOR-capable APs, we recommend that you disable the Admin status of the XOR radio using the **Configure Access Points** workflow. The Admin status configured using the **Configure Access Points** workflow isn't overwritten when the wireless controller or APs are reprovisioned. For more information, see Configure APs, on page 1382.

b) Under **Parent Profile**, click **High**, **Medium (Typical)**, **Low**, or **Custom**. (The available data rates and power configuration values change depending on the parent profile chosen. For example, if you choose **High**, it populates the profile configurations available in the device for 2.4-GHz. If you change any settings in the populated data rates and power configurations, the **Parent Profile** automatically changes to **Custom**.) A new RF profile is created only for the selected custom profiles.

Note **Low**, **Medium (Typical)**, and **High** are the default RF profiles. If you choose a default RF profile, the respective RF profile on the device is used, and the new RF profile isn’t created on wireless controller.

c) **DCA Channel** dynamically manages the channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.

- Check the **Select All** check box to select DCA channels **1**, **6**, and **11**. Alternatively, check the individual check boxes next to the channel numbers.
- If the individual channel numbers aren't already displayed, click **Show Advanced** to select the channel numbers under the **Advanced Options**.
- Check the **Select All** check box to select DCA channels that are under **Advanced Options**, or check the check box next to the individual channel numbers. The available channel numbers are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

Note

- For Cisco AireOS Wireless Controller, Catalyst Center automatically configures the selected DCA channels in the global RRM DCA channel list.
- Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

d) Under **Supported Data Rate**, do this configuration:

- Check the **Enable 802.11b data rates** check box to enable the 802.11b data rates. This action also enables the 802.11b supported data rate check boxes in the **Mandatory Data Rates** area.
- Use the slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

e) Under **Mandatory Data Rates**, check the check boxes next to the individual data rates. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

If you enable 802.11b data rates, **1**, **2**, and **5.5** data rates are also available.

f) Under **Tx Power Configuration**, set the power level and power threshold for an AP.

- **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm to 30 dBm.
- **RX SOP Threshold (dBm)**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 2.4-GHz band, the high threshold value is -79 dBm, the medium threshold value is -82 dBm, and the low threshold value is -85 dBm.
- **TPC Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase or decrease the power value,

which causes the AP to operate at higher or lower transmission power rates. The range is from -80 dBm to -50 dBm.

g) Under **Coverage Hole Detection**, do this configuration:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for the RRM general parameters, see Create a feature template for RRM general parameters, on page 528. For information about provisioning, see Provision Wireless Devices, on page 617.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

h) Under **Client Limit**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note A maximum client limit isn't supported on Cisco AireOS Wireless Controllers.

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

i) Under **802.11ax**, configure this spatial reuse parameters for 802.11ax:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.

- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 5 Do this configuration in the **5 GHz** tab:

a) Ensure that the **5 GHz** toggle button is enabled.

Note
- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **5 GHz** toggle button, Catalyst Center disables the Admin status of the **5 GHz** RF profile.
- For Cisco AireOS Wireless Controller, if you disable the **2.4 GHz** toggle button and reprovision the wireless controller or AP, Catalyst Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of the corresponding radios on the APs.
- For Cisco AireOS Wireless Controller, when you disable the Admin status for the 5-GHz band on the RF profile, Catalyst Center changes the XOR radio on the APs using that RF profile to manual 2.4-GHz mode. If you enable the Admin status later and reprovision the AP, Catalyst Center changes the radio to automatic mode enabling the usage of 2.4-GHz and 5-GHz bands, and monitor mode. So, if you want to disable the Admin status for the 5-GHz band on XOR-capable APs, we recommend that you disable the Admin status of the XOR radio using the **Configure Access Points** workflow. The Admin status configured using the **Configure Access Points** workflow isn't overwritten when the wireless controller or APs are reprovisioned. For more information, see Configure APs, on page 1382.

b) Under **Parent Profile**, click **High**, **Medium (Typical)**, **Low**, or **Custom**. (The available data rates and power configuration values change depending on the parent profile chosen. For example, if you choose **High**, it populates the configurations available in the device for 5 GHz. If you change any settings in the populated data rates and power configurations, the **Parent Profile** automatically changes to **Custom**.) A new RF profile is created only for select custom profiles.

Note **Low**, **Medium (Typical)**, and **High** are the default RF profiles. If you choose a default RF profile, the respective RF profile that is already present in the device is used and the new RF profile isn't created on wireless controller.

c) From the **Channel Width** drop-down list, choose a channel bandwidth option: **20 MHz**, **40 MHz**, **80 MHz**, **160 MHz**, or **Best**.

Note For wireless controllers that are running Cisco IOS XE Release 26.2.1 and later, channel width is replaced by the DBS channel width. For these wireless controllers, use the **DBS Channel Width** slider.

d) Use the **DBS Channel Width** slider to set the minimum and maximum channel width of the RF profile for wireless controllers that are running Cisco IOS XE Release 26.2.1 and later.

The available channel width options are **20 MHz**, **40 MHz**, **80 MHz**, and **160 MHz**.

e) To enable preamble puncturing for this band, click the **Preamble Puncturing** toggle button.



Note Preamble puncturing is applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

f) Check the **Zero Wait DFS** check box to allow APs with 5-GHz radio band to switch to a new channel without any waiting time.



Note Catalyst Center supports Zero Wait DFS for Cisco Wireless Controllers running Cisco IOS XE Release 17.9.1 and later.

g) Under **DCA Channel**, do this configuration to manage the channel assignments:



Note For Cisco AireOS Wireless Controller, Catalyst Center automatically configures the selected DCA channels in the global RRM DCA channel list.

Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- Check the **Select All** check box to select DCA channels **UNII-1 36-48**, **UNII-2 52-144**, and **UNII-3 149-173**. Alternatively, check the individual check boxes next to the channel numbers.
- If the individual channel numbers aren't already displayed, click **Show Advanced** to choose the channel numbers for each band.
- **UNII-1 36-48**: The channels available for UNII-1 band are **36**, **40**, **44**, and **48**. Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
- **UNII-2 52-144**: The channels available for UNII-2 band are **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **120**, **124**, **128**, **132**, **136**, **140**, and **144**. Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.
- **UNII-3 149-173**: The channels available for UNII-3 band are **149**, **153**, **157**, **161**, **165**, **169**, and **173**. Check the **UNII-3 149-173** check box to include all channels, or check an individual check box.

h) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

i) Under **Mandatory Data Rates**, check the check boxes next to the individual data rates. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

j) Under **Tx Power Configuration**, set the power level and power threshold for an AP.

- **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm to 30 dBm, and the default is -10 dBm.
- **RX SOP Threshold (dBm)**: RX SOP determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 5-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.
- **TPC Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase or decrease the power value, which causes the AP to operate at higher or lower transmission power rates. The range is from -50 dBm to 80 dBm, and the default threshold is -70 dBm.

k) Under **Coverage Hole Detection**, do this configuration:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for the RRM general parameters, see Create a feature template for RRM general parameters, on page 528. For information about provisioning, see Provision Wireless Devices, on page 617.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

l) Under **Client Limit**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note A maximum client limit isn't supported on Cisco AireOS Wireless Controllers.

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

m) Under **Flexible Radio Assignment (FRA)**, check the **Client Aware** check box to enable the Client Aware feature.

This feature monitors the dedicated 5-GHz radio. When the client load passes the threshold, it automatically changes the FRA from a monitor role into a 5-GHz role, effectively doubling the capacity of the cell on demand. Once the capacity crisis is over and Wi-Fi load returns to normal, the radios resume their previous roles.

Note You must enable FRA in **Design** > **Feature Templates** > **Wireless** > **RRM FRA Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for the RRM FRA parameters, see Create a feature template for RRM FRA parameters, on page 527. For information about provisioning, see Provision Wireless Devices, on page 617.

If you enable the Client Aware feature, do this configuration:

- In the **Client Select (%)** field, enter a value for client selection. The valid range is from 0 through 100 percent. The default value is 50 percent.
- In the **Client Reset (%)** field, enter a reset value for the client. The valid range is from 0 through 100 percent. The default value is 5 percent.

n) Under **802.11ax**, configure this spatial reuse parameters for 802.11ax:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 6 Configure these in the **6 GHz** tab:

a) Ensure that the **6 GHz** toggle button is enabled.

Note
- The 6-GHz radio is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **6 GHz** toggle button, Catalyst Center disables the Admin status of the **6 GHz** RF profile.

b) Use the **DBS Channel Width** slider to set the minimum and maximum channel width of the RF profile.

The available channel width options are **20 MHz**, **40 MHz**, **80 MHz**, **160 MHz**, or **320 MHz**.

Note The 320 MHz channel width is applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

c) To enable preamble puncturing for this band, click the **Preamble Puncturing** toggle button.

Note Preamble puncturing is applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

d) Enable the **Enable PSC Enforcing** toggle button to allow Preferred Scanning Channel (PSC) enforcement.

PSC enforcement improves the connectivity of 6-GHz devices by prioritizing PSC-enabled channels.

Note If you enable PSC enforcement, the check boxes next to the non-PSC channels are dimmed.

e) Under **DCA Channel**, do this configurration to manage channel assignments.

- Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.
  - **UNII-5 1-93**
  - **UNII-6 97-113**
  - **UNII-7 117-185**
  - **UNII-8 189-233**
- If the channel numbers aren't already displayed, click **Show Advanced** to select the channel numbers for each band.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

f) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

g) Under **Mandatory Data Rates**, check the check boxes next to the individual data rates. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

h) Under **Tx Power Configuration**, set the power level and power threshold for an AP.

- **Standard Power Service**: For APs with the standard power capability, compliance with FCC regulations requires the activation of Automatic Frequency Coordination (AFC). AFC uses the AP location and height data to determine the optimal channel and transmission power, ensuring noninterference with the licensed incumbent users on the 6-GHz band. You can use the Standard Power Service feature on Catalyst Center to activate AFC. By default, this feature is disabled. To enable this feature, click the **Standard Power Service** toggle button.

  This feature is applicable only for Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.12.3 or later. When this feature is disabled, the 6-GHz dual-power mode APs are restricted to operate only in the low-power indoor mode, and the standard-power mode only APs have the radios disabled completely.

  Note To ensure proper functioning of this feature, you must configure the AP height, AP height uncertainty, and external antenna cable length on the corresponding wireless controller. For the standard power-capable APs to operate on standard power, you must ensure that you select at least one supported DCA channel based on your country-specific regulations.

- **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm to 30 dBm.

- **RX SOP Threshold (dBm)**: RX SOP determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 6-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.

- **TPC Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase or decrease the power value, which causes the AP to operate at higher or lower transmission power rates. The range is from -80 dBm to -50 dBm.

i) Under **Coverage Hole Detection**, do this configuration:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for the RRM general parameters, see Create a feature template for RRM general parameters, on page 528. For information about provisioning, see Provision Wireless Devices, on page 617.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

j) Under **Client Limit**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note
- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

k) Under **Flexible Radio Assignment (FRA)**, complete this task:

Note
- You must enable FRA in **Design** > **Feature Templates** > **Wireless** > **RRM FRA Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for the RRM FRA parameters, see Create a feature template for RRM FRA parameters, on page 527. For information about provisioning, see Provision Wireless Devices, on page 617.
- FRA is supported only on wireless controllers that run Cisco IOS XE Release 17.9.1 or later.

- In the **Client Reset Count** field, enter a reset count value for the client. The valid range is from 0 through 10. The default value is 1.
- In the **Client Utilization Threshold (%)** field, enter a utilization threshold value for the client. The valid range is from 0 through 100 percent. The default value is 5 percent.

l) Under **802.11ax**, do this configuration:

- From the **6 GHz Discovery Frames** drop-down list, choose the required option from **None**, **Broadcast Probe Response**, and **FILS Discovery**.

  6-GHz discovery frames are needed if the 6-GHz band is the only operational band. For more information about the 6-GHz discovery frames, click **Learn More**.

- In the **Broadcast Probe Response Interval (msec)** field, enter the broadcast probe response interval, in msec. The valid range is from 5 msec through 25 msec. The default value is 20 msec.

m) Under **MULTI BSSID**, check the check box to enable these multiple basic service set identifier (BSSID) parameters:

- Target Wake time
- TWT Broadcast Support



Note You must enable multiple BSSID in **Design** > **Feature Templates** > **Wireless** > **Dot11ax Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for Dot11ax, see Create a feature template for Dot11ax configuration, on page 519. For information about provisioning, see Provision Wireless Devices, on page 617.

n) Under **802.11AX PARAMETERS**, check the corresponding check box to enable these parameters:

- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO



Note Starting with Cisco IOS XE Release 17.18.2, these configurations are also used for the corresponding 802.11be configurations on the 6-GHz radio band.

o) Under **802.11BE PARAMETERS**, check the corresponding check box to enable these parameters:

- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO
- OFDMA Multi-RU

Note The 802.11be parameters are applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

Starting with Cisco IOS XE Release 17.18.2, the **OFDMA Uplink**, **OFDMA Downlink**, **MU-MIMO Uplink**, and **MU-MIMO Downlink** configurations are deprecated and ignored under this section. To configure these settings, use the **802.11AX PARAMETERS** section.

You must enable the 802.11be status in **Design** > **Feature Templates** > **Wireless** > **Dot11be Status Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for 802.11be, see Create a feature template for Dot 11be status configuration, on page 521. For information about provisioning, see Provision Wireless Devices, on page 617.

p) Under **SPATIAL REUSE**, do this configuration:

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 7 Click **Save**.

Step 8 (Optional) To mark a profile as the default RF profile, check the **Profile Name** check box and click **Mark Default**. In the **Warning** window, click **OK**.

What to do next

You must provision the APs to apply the RF profile settings on the device. For more information, see Provision Cisco APs on day 1, on page 627.

Edit or delete a basic radio frequency profile

This procedure describes how to edit or delete a basic RF profile.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Wireless Radio Frequency Profile** area, click the **Basic RF Profile** tab.

Note The **Basic RF Profile** table lists the number of created basic RF profiles based on **Profile Name**, **Type**, **2.4 GHz Data Rates**, **5 GHz Data Rates**, **6 GHz Data Rates**, **Channel Width**, and **Profile Type**.

Step 6 Check the check box next to the basic profile name that you want to edit.

Step 7 From the **Action** drop-down list, choose **Edit/View**.

Note You can edit one basic RF profile at a time.

Step 8 In the **Edit Wireless Radio Frequency Profile** window, configure the basic RF profile settings. For more information, see Create a wireless radio frequency profile, on page 383.

Step 9 Click **Save**.

Step 10 To delete a basic RF profile, check the check box next to the basic RF profile name.

Step 11 From the **Action** drop-down list, choose **Delete** and then click **Yes**.

Step 12 To mark a basic RF profile as the default, check the check box next to a basic RF profile name.

Step 13 From the **Action** drop-down list, choose **Mark Default** and then click **Yes**.

What to do next

For Cisco AireOS Wireless Controllers, if you modify the DCA channels or data rates for an RF profile that is already provisioned on a wireless controller, Catalyst Center resets the corresponding radio.

If you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovision also pushes the RF profile updates to the devices and reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Clone a basic radio frequency profile

You can create a copy of a basic RF profile by cloning it. Cloning allows you to reuse the configurations of an existing RF profile for a new RF profile. You can clone both the system and custom RF profiles.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Basic RF Profile** tab, check the check box next to the profile name that you want to clone.

Step 6 From the **Actions** drop-down list, choose **Create a Clone**.

Step 7 In the **Profile Name** field of the **Create Wireless Radio Frequency Profile** window, enter a unique name for the profile.

Step 8 Edit the RF profile configurations as necessary. For more information, see Create a wireless radio frequency profile, on page 383.

Step 9 Click **Save**.

Prerequisites for configuring AI radio frequency profiles

- You must enable Cisco AI Network Analytics under the system settings. For more information, see **Configure Cisco AI Network Analytics Data Collection** in the *Cisco Catalyst Center Administrator Guide*.
- You must enable AI-Enhanced RRM. From the main menu, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**. In the **AI-ENHANCED RRM** area of the **Cisco AI Analytics** window, click the toggle button to enable the AI-Enhanced RRM.
- AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.7.1 or later.



Note Ensure that the **Group Mode** option for all the three bands (2.4 GHz, 5 GHz, and 6 GHz) is configured as **auto** or **leader** on the wireless controller.

- AI RF profiles are supported for 6-GHz radio only on wireless controllers that run Cisco IOS XE Release 17.9.1 and later.
- For a deployment without device provisioning, to enable and push the AI RF profile to a site, you must assign APs to the sites where you want to configure the AI-Enhanced RRM.
- You must be a **Super Admin** or **Network Admin**.

Create an AI radio frequency profile

This procedure describes how to create an AI radio frequency profile for your building or a standalone outdoor area.

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Wireless Radio Frequency Profile** area, hover your cursor over **Add** and choose **AI RF Profile**.

Step 6 In the **Profile Name** field of the **Create AI Radio Frequency Profile** window, enter the RF profile name.

Step 7 In the **Radio Frequency Settings** area of **Basic Settings**, check the **2.4 GHz**, **5 GHz**, or **6 GHz** check box.

The RF bands are checked by default. If you uncheck a band, Catalyst Center disables the Admin status of the corresponding RF profile.

Note Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.9.1 and later support the AI RF profile for the **6 GHz** band.

Step 8 In the **Busy Hours** area, define the start and end time of the site time zone.

Note Busy hours are dependent upon the time zone of the site. You must configure a time zone for the respective site under network settings.

Step 9 In the **Busy Hour Sensitivity** area, click the **Low**, **Medium**, or **High** radio button to define the threshold of the Radio Resource Management (RRM) sensitivity for the busy hours interval.

Step 10 In the **Enable RF Settings** area, click the toggle buttons under the **2.4 GHz**, **5 GHz**, or **6 GHz** columns to enable or disable RF settings for the corresponding bands.

The supported RF settings are:

- **Flexible Radio Assignment (FRA)**: FRA optimizes the radio coverage per band and determines the best role assignment for redundant radios.
- **Dynamic Channel Assignment (DCA)**: DCA dynamically manages the channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.
- **Transmit Power Control (TPC)**: TPC manages and transmits power for APs. It also maximizes the SNR during the reduction in interference.
- **Dynamic Bandwidth Selection (DBS)**: DBS monitors and adjusts the channel width to balance performance and interference.

Note

- When you disable the **2.4 GHz** band for FRA, it automatically disables the **5 GHz** band for FRA, and conversely.
- When you disable the **5 GHz** band for DCA, it disables the **2.4 GHz** band for FRA and the **5 GHz** band for FRA and DBS.
- You can individually enable the **2.4 GHz** band for DCA and TPC, and the **5 GHz** band for DCA, TPC, and DBS. For the **5 GHz** band, if DCA and DBS are disabled and you enable DBS, DCA is also enabled.
- You can enable or disable the **6 GHz** band together for DCA and DBS RF settings. You can individually enable the **6 GHz** band for TPC.
- FRA isn't supported for the **6 GHz** band.

Step 11 In the **Advanced** area, click the **2.4 GHz** toggle button.

a) In the **DCA Channel** area, check the **Select All** check box to select DCA channels **1**, **6**, and **11**. Alternatively, check the individual check boxes next to the channel numbers.

b) In the **Advanced Options** area, check the **Select All** check box to select all the DCA channels.

c) If the individual channel numbers aren't already displayed, click **Show Advanced** to select the remaining channel numbers.

d) Check the check box next to the individual channel numbers. The channel numbers that are available for the profile are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

e) In the **Supported Data Rate** area, do this configuration:

- Check the **Enable 802.11b data rates** check box to enable the 802.11b data rates. This action also enables the 802.11b supported data rate check boxes in the **Mandatory Data Rates** area.
- Use the slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

f) In the **Mandatory Data Rates** area, check the check box next to the individual data rates. The available data rates are **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

If you enable 802.11b data rates, **1**, **2**, and **5.5** data rates are also available.

g) In the **Tx Power Configuration** area, do this configuration:

- **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm through 30 dBm. The minimum default is -10 dBm and the maximum default is 30 dBm.

- **RX SOP Threshold (dBm)**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 2.4-GHz band, the high threshold value is -79 dBm, the medium threshold value is -82 dBm, and the low threshold value is -85 dBm.

- **TPC Power Threshold**: Is the cutoff signal level used by RRM to determine whether to reduce the power of an AP. Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmission power rates. The range is from -80 dBm through -50 dBm.

h) Under **Coverage Hole Detection**, do this configuration:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for RRM general parameters, see Create a feature template for RRM general parameters, on page 528. For information about provisioning, see Provision Wireless Devices, on page 617.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

i) Under **CLIENT LIMIT**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note
- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

j) Under **802.11ax**, configure these spatial reuse parameters:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 12 In the **Advanced** area, click the **5 GHz** toggle button.

a) (Optional) If you disable DBS for this band, from the **Channel Width** drop-down list, choose a channel bandwidth option: **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**.

b) (Optional) If you enable DBS for this band, use the **DBS Channel Width** slider to set the minimum and maximum channel width of the AI RF profile.

The available channel width options are **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**.

The **Auto Channels Logic** area displays a color-coded representation of channels that are available in the Unlicensed National Information Infrastructure (UNII) radio bands for the available channel widths.

Note This option is supported on wireless controllers that are running Cisco IOS XE Release 26.2.1 and later.

c) To enable preamble puncturing on the band, click the **Preamble Puncturing** toggle button.

Note Preamble puncturing is applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

d) Check the **Zero Wait DFS** check box to allow APs with 5-GHz radio to switch to a new channel without any waiting time.

Note Catalyst Center supports Zero wait DFS for Cisco Wireless Controllers running Cisco IOS XE Release 17.9.1 and later.

e) Set the **DCA Channel** to manage these channel assignments:

- **UNII-1 36-48**: The channels available for UNII-1band are **36**, **40**, **44**, and **48**.

- **UNII-2 52-144**: The channels available for UNII-2band are **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **120**, **124**, **128**, **132**, **136**, **140**, and **144**.
- **UNII-3 149-165**: The channels available for UNII-3 band are **149**, **153**, **157**, **161**, and **165**.

f) Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.

g) Click **Show Advanced** to view and select the individual DCA channel numbers.

- Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
- Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.
- Check the **UNII-3 149-165** check box to include all channels, or check an individual check box.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

h) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

i) In the **Mandatory Data Rates** area, check the check box next to the individual data rates. The available data rates are **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.

j) In the **Tx Power Configuration** area, do this configuration:

- Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm through 30 dBm. The minimum default is -10 dBm and the maximum default is 30 dBm.
- **RX SOP Threshold (dBm)**: RX SOP determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 5-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.
- Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -80 dBm through -50 dBm.

k) Under **Coverage Hole Detection**, do this configuration:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for RRM general parameters, see Create a feature template for RRM general parameters, on page 528. For information about provisioning, see Provision Wireless Devices, on page 617.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

l) Under **CLIENT LIMIT**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note
- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

m) Under **802.11ax**, configure these spatial reuse parameters:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.

  SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 13 In the **Advanced** area, click the **6 GHz** toggle button.

a) Use the **DBS Channel Width** slider to set the minimum and maximum channel width of the AI RF profile.

The available channel width options are **20 MHz**, **40 MHz**, **80 MHz**, **160 MHz**, or **320 MHz**.

Note The 320 MHz channel width is applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

The **Auto Channels Logic** area displays a color-coded representation of channels that are available in the UNII radio bands for the available channel widths.

You can select **DBS Channel Width** only when DBS is enabled.

b) To enable preamble puncturing on the band, click the **Preamble Puncturing** toggle button.

Note Preamble puncturing is applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

c) Enable the **Enable PSC Enforcing** toggle button to allow Preferred Scanning Channel (PSC) enforcement.

PSC enforcement improves the connectivity of the 6-GHz devices by prioritizing the PSC-enabled channels.

Note If you enable PSC enforcement, the check boxes next to the non-PSC channels are dimmed and the check boxes next to the PSC channels are checked by default. If necessary, you can uncheck the check box next to the required PSC channel.

d) Set the **DCA Channel** to manage these channel assignments:

- **UNII-5 1-93**: The channels available for the UNII-5 band are **1**, **5**, **9**, **13**, **17**, **21**, **25**, **29**, **33**, **37**, **41**, **45**, **49**, **53**, **57**, **61**, **65**, **69**, **73**, **77**, **81**, **85**, **89**, and **93**.
- **UNII-6 97-113**: The channels available for the UNII-6 band are **97**, **101**, **105**, **109**, and **113**.
- **UNII-7 117-185**: The channels available for the UNII-7 band are **117**, **121**, **125**, **129**, **133**, **137**, **141**, **145**, **149**, **153**, **157**, **161**, **165**, **169**, **173**, **177**, **181**, and **185**.
- **UNII-8 189-233**: The channels available for the UNII-8 band are **189**, **193**, **197**, **201**, **205**, **209**, **213**, **217**, **221**, **225**, **229**, and **233**.

e) Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.

f) Click **Show Advanced** to select the remaining DCA channel numbers.

- Check the **UNII-5 1-93** check box to include all channels, or check an individual check box.
- Check the **UNII-7 117-185** check box to include all channels, or check an individual check box.
- Check the **UNII-8 189-233** check box to include all channels, or check an individual check box.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

g) Use the **Supported Data Rates** slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

h) In the **Mandatory Data Rates** area, check the check box next to the individual data rates. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.

i) In the **Tx Power Configuration** area, do this configuration.

- **Standard Power Service**: For APs with the standard power capability, compliance with FCC regulations requires the activation of Automatic Frequency Coordination (AFC). AFC uses the AP location and height data to determine the optimal channel and transmission power, ensuring noninterference with the licensed incumbent users on the 6-GHz band. You can use the Standard Power Service feature on Catalyst Center to activate AFC. By default, this feature is disabled. To enable this feature, click the **Standard Power Service** toggle button.

  This feature is applicable only for Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.12.3 or later. When this feature is disabled, the 6-GHz dual-power mode APs are restricted to operate only in the low-power indoor mode, and the standard-power mode only APs have the radios disabled completely.

  Note To ensure proper functioning of this feature, you must configure the AP height, AP height uncertainty, and external antenna cable length on the corresponding wireless controller. For the standard power-capable APs to operate on standard power, you must ensure that you select at least one supported DCA channel based on your country-specific regulations.

- Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm through 30 dBm.
- **RX SOP Threshold (dBm)**: RX SOP determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP Threshold (dBm)** drop-down list, choose **High**, **Medium**, **Low**, **Auto**, or **Custom** threshold value.

  If you choose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 dBm through -60 dBm. For the 6-GHz band, the high threshold value is -76 dBm, the medium threshold value is -78 dBm, and the low threshold value is -80 dBm.
- Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -80 dBm through -50 dBm.

j) Under **Coverage Hole Detection**, do this configuration:

Note You must enable global coverage hole detection in **Design** > **Feature Templates** > **Wireless** > **RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for RRM general parameters, see Create a feature template for RRM general parameters, on page 528. For information about provisioning, see Provision Wireless Devices, on page 617.

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

k) Under **CLIENT LIMIT**, in the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note
- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

l) Under **802.11ax**, do this configuration:

- From the **6 GHz Discovery Frames** drop-down list, choose the required option from **None**, **Broadcast Probe Response**, and **FILS Discovery**.

  6-GHz discovery frames are needed if the 6-GHz band is the only operational band. For more information about the 6-GHz discovery frames, click **Learn More**.
- In the **Broadcast Probe Response Interval (msec)** field, enter the broadcast probe response interval, in msec. The valid range is from 5 msec through 25 msec. The default value is 20 msec.

m) Under **MULTI BSSID**, check the check box to enable the multiple basic service set identifier (BSSID) parameters, including:

- Target Wake time
- TWT Broadcast Support

Note You must enable multiple BSSID in **Design** > **Feature Templates** > **Wireless** > **Dot11ax Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for Dot11ax, see Create a feature template for Dot11ax configuration, on page 519. For information about provisioning, see Provision Wireless Devices, on page 617.

n) Under **802.11AX PARAMETERS**, check the corresponding check box to enable these parameters:

- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO

Note Starting with Cisco IOS XE Release 17.18.2, these configurations are also used for the corresponding 802.11be configurations on the 6-GHz radio band.

o) Under **802.11BE PARAMETERS**, check the corresponding check box to enable these parameters:

- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO
- OFDMA Multi-RU

Note The 802.11be parameters are applicable only for Cisco Wireless Controllers running Cisco IOS XE 17.15.2 or later.

Starting with Cisco IOS XE Release 17.18.2, the **OFDMA Uplink**, **OFDMA Downlink**, **MU-MIMO Uplink**, and **MU-MIMO Downlink** configurations are deprecated and ignored under this section. To configure these settings, use the **802.11AX PARAMETERS** section.

You must enable the 802.11be status in **Design** > **Feature Templates** > **Wireless** > **Dot11be Status Configuration** for the corresponding radio band and provision it on the managing wireless controller. For information about the feature template for 802.11be, see Create a feature template for Dot 11be status configuration, on page 521. For information about provisioning, see Provision Wireless Devices, on page 617.

Step 14 Click **Save**.

What to do next

You must provision the APs to apply the RF profile settings on the device. For more information, see Provision Cisco APs on day 1, on page 627.

Edit an AI radio frequency profile

This procedure describes how to edit an AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.

The **AI RF Profile** table lists the number of created AI RF profiles based on **Profile Name**, **Busy Hours**, **Busy Hour Sensitivity**, **FRA**, **DCA**, **DBS**, **TPC**, and **Mapped Buildings**.

Step 6 Check the check box next to the AI RF profile that you want to edit.

You can edit one AI RF profile at a time.

Step 7 Click **Edit/View**.

Step 8 In the **Edit AI RF Profile** window, configure the AI RF profile settings. For more information, see Create an AI radio frequency profile, on page 396.

Step 9 Click **Save**.

What to do next

If you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovision also pushes the RF profiles updates to the devices and reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Delete an AI radio frequency profile

This procedure describes how to delete an AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.

The **AI RF Profile** table lists the number of created AI RF profiles based on **Profile Name**, **Busy Hours**, **Busy Hour Sensitivity**, **FRA**, **DCA**, **DBS**, **TPC**, and **Mapped Buildings**.

Step 6 To delete an AI RF profile, check the check box next to the AI RF profile that you want to delete.

Step 7 Click **Delete** and then click **Yes**.



Note Catalyst Center does not allow you to delete an AI RF Profile, which is already assigned to a building.

What to do next

If you delete an RF profile that is already provisioned on a wireless controller and AP, you must reprovision the wireless controller. Reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Clone an AI radio frequency profile

You can create a copy of an AI RF profile by cloning it. Cloning allows you to reuse the configurations of an existing AI RF profile for a new AI RF profile.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 Click the **AI RF Profile** tab.

Step 6 Check the check box next to the profile name that you want to clone.

Step 7 Click **Create a Clone**.

Step 8 In the **Profile Name** field of the **Create AI Radio Frequency Profile** window, enter a unique name for the profile.

Step 9 Edit the RF profile configurations as necessary. For more information, see Create an AI radio frequency profile, on page 396.

Step 10 Click **Save**.

Configure AI-Enhanced RRM

Use this procedure to assign an AI RF profile to a building.

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure AI-Enhanced RRM**.

Step 2 In the **Configure AI-Enhanced RRM** window, click **Let's Do it** to go directly to the workflow.

Step 3 In the **Task Name** field of the **Get Started** window, enter a task name.

Step 4 In the **Select Deployment Type** window, choose the deployment type from the available options (**Enable Without Device Provisioning** and **Enable with Device Provisioning**).

Step 5 In the **AI-Enhanced RRM Prerequisites** window, review the prerequisites to configure AI-enhanced RRM and ensure that required configurations are completed.

(Optional) Click the link in the cards to update the corresponding configurations. If you update these configurations, refresh the card to view the updated status.

Step 6 In the **Select Locations to Assign AI-RF Profiles** window, choose the locations where you want to assign the AI-enabled RF profiles.

You can either search for a site by entering its name in the **Search Hierarchy** field, or expand **Global** and choose the sites.

The **Site selection summary** table displays:

- Selected sites
- Primary wireless controller that manages the location
- Secondary wireless controller assigned to provide redundancy for the location
- Impacted locations that are managed by the selected wireless controller.

Enabling AI-enhanced RRM on the wireless controller enables it on all sites managed by the wireless controller.

For example, if a wireless controller manages three buildings and you enable AI RF profile on one building, Catalyst Center automatically enables the same AI RF profile on the other two buildings.

If you choose the **Enable Without Device Provisioning** deployment type, complete these configurations:

a) Assign primary wireless controller for all locations.

1. Check the check box for the required locations.
2. Click **Assign/Update Primary WLC**.

3. In the **Assign Primary Wireless Controller** dialog box, select a deployment type.

If you choose...	Then...
the **All floors are managed by the same wireless controller** option	Select the required wireless controller.
the **Some floors are managed by different wireless controller(s)** option	**a.** Check the check box for the required floors. **b.** Click **Assign Primary WLC**. **c.** In the **Assign Primary Wireless Controller for floor(s)** dialog box, select the required wireless controller. **d.** Click **Assign**.

4. Click **Confirm**.

b) (Optional) Assign secondary wireless controller for a location.

1. Check the check box for the required locations.
2. Click **Assign/Update Secondary WLC**.
3. In the **Assign Secondary Wireless Controller** dialog box, select a deployment type.

If you choose...	Then...
the **All floors are managed by the same wireless controller** option	Select the required wireless controller.
the **Some floors are managed by different wireless controller(s)** option	**a.** Check the check box for the required floors. **b.** Click **Assign Secondary WLC**. **c.** In the **Assign Secondary Wireless Controller for floor(s)** dialog box, select the required wireless controller. **d.** Click **Assign**.

4. Click **Confirm**.



Note The primary and secondary wireless controllers must be different.

Step 7 Choose AI RF profile to assign to the locations.

If you choose...	Then...
the **Enable Without Device Provisioning** deployment type	In the **Assign AI RF Profile and Verify Tags** window. **a.** In the **Sites** table, choose an AI RF profile from the drop-down list under **Select the AI RF profile** for the location. **b.** Click the ellipsis icon under the **Actions** column to create an AI RF profile, copy the existing RF profile, or apply the RF profile to all locations. You can also create an AI RF profile using the **Create New AI RF Profile** option. For more information, see Create an AI radio frequency profile, on page 396. **c.** Verify the RF tags assigned to each location. Catalyst Center associates the selected RF tag with the configured RF tag. We recommend that you create unique RF tags for the wireless controller across APs on different locations. Unique RF tags allow you to apply actionable insights generated from AI-enhanced RRM to each location.
the **Enable With Device Provisioning** deployment type	In the **Assign AI RF Profile** window. **a.** In the **Sites** table, choose an AI RF profile from the drop-down list under **Select the AI RF profile** for the location. **b.** Click the ellipsis icon under the **Actions** column to create an AI RF profile, copy the existing RF profile, or apply the RF profile to all locations. You can also create an AI RF profile using the **Create New AI RF Profile** option. For more information, see Create an AI radio frequency profile, on page 396.

Step 8 In the **Details of selected AI RF Profiles** window, review the **AI Settings**, **Common Settings**, and **Assignment** details of the AI-enabled RF profiles.

Note AI-Enhanced RRM computation occurs every 30 minutes. RRM decisions are updated and pushed to devices after the computation.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note In the **Download a backup of current RF settings** dialog box, you can download a backup CSV file that contains the selected buildings' current RF configuration details. When you're ready, click **Confirm** to continue.

If you disable AI-Enhanced RRM later, you can use this backup CSV file to update the RF profile configurations. For more information, see Unassign a location from an existing AI RF profile, on page 413.

Step 11 On the **Tasks** window, monitor the task deployment.

Assign a location to an existing AI RF profile

This procedure describes how to assign a location to an existing AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.
The **AI RF Profile** table lists the number of created AI RF profiles.

Step 6 Click the three dots under the **Action** column for an AI RF profile.

Step 7 From the drop-down list, choose **Assign Location**.

The **Manage Location Assignment** window opens.

Step 8 You can either search for a site by entering its name in the **Search** field, or expand **All Sites** to choose the sites.

Note
- The site hierarchy shows the AI-enabled locations.
- Sites or buildings that are not eligible for the AI profile are disabled.
- You cannot select a floor under a building. When you select a building for an AI-enabled RF profile, the floors underneath are assigned automatically.

If the same wireless controller manages other buildings, the **Confirm Impacted Sites** window opens.

Step 9 Review the confirmation and click **Confirm** to assign the chosen sites to the AI-enabled RF profile.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.



Note In the **Download a backup of current RF settings** dialog box, you can download a backup CSV file that contains the selected buildings' current RF configuration details. When you're ready, click **Confirm** to continue.

If you disable AI-Enhanced RRM later, you can use this backup CSV file to update the RF profile configurations. For more information, see Unassign a location from an existing AI RF profile, on page 413.

Step 11 On the **Tasks** window, monitor the task deployment.

What to do next

Provision Devices of an AI RF Profile-Enabled Building

This procedure describes how to provision devices across the locations to deploy the AI RF profile.

1. From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

   In the **Inventory** window, the **Device** table lists the discovered AI RF profile associated devices.
2. Check the check box next to the AI RF profile associated device name that you want to provision.
3. From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
4. Proceed through all the steps and in the **Summary** step, click **Deploy**.
5. In the **Summary** window, view the remaining network settings that will be pushed to the device. For more information, see Wireless device provisioning overview, on page 617.

Unassign a location from an existing AI RF profile

This procedure describes how to unassign a location from an existing AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.
The **AI RF Profile** table lists the number of created AI RF profiles.

Step 6 Click the ellipsis icon under the **Action** column for an AI RF profile and choose **Unassign Locations**.

The **Unassign AI RF Profile** window opens.

Step 7 In the **Task Name** field of the **Task Name** window, enter a task name.

Step 8 In the **Select Locations to Disable AI-Enhanced RRM** window, choose the location to unassign an AI RF profile.

Step 9 In the **Select Replacement RF Profiles for Provisioned Buildings** window, select a replacement RF profile for provisioned buildings.

Note If there are no applicable buildings, skip to next step.

Use one of these options to select the RF profile:

- **Select from Available Basic RF Profiles**: From the drop-down list, choose a wireless RF profile.

  Note If APs are associated with AP zones, the wireless RF profile defined in the AP zone takes precedence over the selected RF profile.

- **Upload CSV with RF Profile configurations**: Upload the RF profile configurations using a comma-separated value (CSV) file.

  a. Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.

  Note You can either upload the CSV file that you downloaded when you assigned the AI RF Profile to these buildings to revert buildings to non-AI settings or download the **Custom CSV file** with metadata based on your selected buildings, enter the wireless RF profile details, and then upload it. The maximum supported file size is 10 MB.

  b. Click **Upload**.

  Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed.

From the uploaded CSV file, if you find an RF setting based on the selected location name, a **Confirm RF Settings for Selected Locations** window shows the **Location** and **Matched RF Profiles**.

Step 10 In the **Select Replacement RF Profiles for Non-Provisioned Buildings** window, select a replacement RF profile for buildings that are not provisioned on Catalyst Center.

Note If there are no applicable buildings, skip to next step.

Use one of these options to select the RF profile:

- **Select from Available Basic RF Profiles**: From the drop-down list, choose a wireless RF profile.

  Note If APs are associated with AP zones, the wireless RF profile defined in the AP zone takes precedence over the selected RF profile.

- **Upload CSV with RF Profile configurations**: Upload the RF profile configurations using a CSV file.

  a. Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.

  Note You can either upload the CSV file that you downloaded when you assigned the AI RF Profile to these buildings to revert buildings to non-AI settings or download the **Custom CSV file** with metadata based on your selected buildings, enter the wireless RF profile details, and then upload it. The maximum supported file size is 10 MB.

  b. Click **Upload**.

  Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed.

From the uploaded CSV file, if you find an RF setting based on the selected location name, a **Confirm RF Settings for Selected Locations** window shows the **Location** and **Matched RF Profiles**.

Step 11 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

What to do next

Provision the devices across the AI RF profile assigned locations to deploy the AI RF profile.

1. From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

In the **Inventory** window, the **Device** table lists the discovered AI RF profile associated devices.

2. Check the check box next to the AI RF profile associated device name that you want to provision.
3. From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
4. Proceed through all the steps and in the **Summary** step, click **Deploy**.
5. In the **Summary** window, review the remaining network settings that will be pushed to the device. For more information, see Wireless device provisioning overview, on page 617.

Upgrade a basic radio frequency profile to an AI radio frequency profile

Before you begin

Ensure that the prerequisites are met. For more information, see Prerequisites for configuring AI radio frequency profiles, on page 396.

To onboard a site in an AI-enhanced RRM service, at least one of these services must be enabled:

- Flexible Radio Assignment (FRA)
- Dynamic Channel Assignment (DCA)
- Transmit Power Control (TPC)
- Dynamic Bandwidth Selection (DBS)

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **RF Profiles**.

Step 5 Check the check box next to the basic RF profile name that you want to upgrade to an AI RF profile.

Step 6 From the **Action** drop-down list, choose **Upgrade to AI**.

Step 7 In the confirmation window, click **Yes**.

Step 8 In the **Edit AI RF Profile** window, configure the AI RF profile settings. For more information, see Create an AI radio frequency profile, on page 396.

Note If the basic RF profile uses the channel width of 320 MHz for the 6-GHz band, it will be changed to 160 MHz in the AI RF profile.

Create an AP authorization list

Catalyst Center allows you to configure a list of authorized APs. Catalyst Center supports these types of AP authorization:

- Local authorization uses the AP MAC address, serial number, or both for authorization against the local database.
- AAA authorization uses a list of AAA servers for authorization.

You can choose the AP authorization list while provisioning the Cisco Wireless Controller. Cisco Wireless Controllers respond only to requests from the APs that are present in the AP authorization list.

Note

- If both MAC address and serial number are required for AP authorization, ensure that both are added to the AP authorization list. If one of these AP entries isn't available in the AP authorization list provisioned for a wireless controller, the corresponding AP can't join the network.
- For a mesh AP (MAP), you must add the MAC address for AP authorization.
- For Cisco AireOS Wireless Controllers, Catalyst Center supports only the MAC address for AP authorization. If you configure both MAC address and serial number, only the MAC address is used for Cisco AireOS Wireless Controllers.
- For Cisco Catalyst 9800 Series Wireless Controllers, Catalyst Center supports the configuration of AP authorization lists only on the wireless controllers running Cisco IOS Release 17.5 and later.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Security Settings**.

Step 5 Click the **AP Authorization List** tab.

Step 6 In the **AP Authorization List** table, click **Add**.

Step 7 In the **List name** field of the **AP Authorization List** slide-in pane, enter a name for the AP authorization list.

Step 8 To configure local authorization:

a) In the **Local Auth** tab, check the **Configure Local Authorization** check box.

b) In the **Type** area, choose an authorization type:

- To use the AP MAC address for authorization, click **Mac Address**.
- To use the AP serial number for authorization, click **Serial Number**.

c) To enter the AP MAC address or serial number data, do one of these tasks:

- To add the MAC address or serial number individually to the authorization list, click **Add**. In the **AP Entry** field, enter the data.

- To upload the CSV file with the data, click **Upload**. In the dialog box, do these steps:

  1. Drag and drop your CSV file into the drag and drop area. Alternatively, click **Choose a file** and browse to select your CSV file stored locally.

  Note If you don't have a CSV file, click **Download** to download a CSV file that you can edit and upload.

  2. Click **Save**.

d) (Optional) To use both the MAC address and serial number for authorization:

1. Click **Mac Address**, and enter the AP MAC address data (8.c, on page 417).
2. Click **Serial Number**, and enter the AP serial number data (8.c, on page 417).

Step 9 To configure AAA authorization:

a) In the **AAA Auth** tab, check the **Configure AAA Authorization** check box.

b) Based on the AP authorization requirement for the AAA server, do one of these tasks:

- If the AAA server uses only the MAC address for AP authorization, check the **Authorize AP against MAC Address** check box.
- If the AAA server uses only the serial number for AP authorization, check the **Authorize AP against Serial Number** check box.
- If the AAA server uses both the MAC address and serial number for AP authentication, check both the **Authorize AP against MAC Address** and **Authorize AP against Serial Number** check boxes.

c) To add AP entries to the AP authorization list, do one of these tasks:

- Click the plus icon next to the required AP entry.
- Click the AP entry and click **Add Selected**.

  Note To choose multiple AP entries, press **Shift**, click the AP entries, and click **Add Selected**.

- To add all the AP entries to the AP authorization list, click **Add All**.

  You can use the **Search** field to filter the AP entries.

Step 10 Click **Save**.

Edit or delete an AP authorization list

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Security Settings**.

Step 5 Click the **AP Authorization List** tab.

Step 6 In the **AP Authorization List** table, check the check box next to the authorization list name that you want to edit or delete.

- To edit the AP authorization list, click **Edit**. In the **AP Authorization List** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see Create an AP authorization list, on page 417.
- To delete the AP authorization list, click **Delete**, and then click **Yes**.

Create an AP LSC renewal profile

Use this procedure to create an AP Locally Significant Certificate (LSC) renewal profile.

A certificate for Plug and Play (PnP) AP authentication is issued for a limited period. An AP LSC renewal profile allows a Cisco Catalyst 9800 Series Wireless Controller to automatically renew the certificate before it expires.

Before you begin

The wireless controller must be running Cisco IOS XE Release 17.17.1 or later.

Procedure

Step 1 Navigate to wireless security settings.

a) From the main menu, choose **Design** > **Network Settings**.
b) Click the **Wireless** tab.
c) From the left hierarchy tree, select **Global**.
d) Click **Security Settings**.
e) Click the **AP LSC Certificate Renewal** tab.



Tip If the window displays the **More** drop-down instead of this tab, hover your cursor over **More** and select this tab.

Step 2 Click **Create Profile** to create an AP LSC renewal profile.

Step 3 In the **Create AP LSC Certificate Renewal Profile** slide-in pane, complete these configurations:

a) In the **Profile Name** field, enter a name for the AP LSC renewal profile.
b) In the **Due Time** field, enter the start time in days for automatic renewal of certificates.

   The default value is 30 days. The valid range is 5 to 60 days.

c) Under **Execution**, select how the certificates are renewed.

   - **Staggered** (recommended): renew certificates for applicable APs in batches to minimize client disruptions. You can configure the percentage of APs that reboot during wireless controller provisioning.
   - **One Shot**: renew certificates for all applicable APs at once, which may result in client disruptions.

     If you select this option, we recommend that you schedule the certificate renewal during less busy hours.

d) (Optional) Under **Scheduler**, check the **Configure Scheduler** check box to configure the required schedule for automatic renewal of certificates.

   By default, the wireless controller automatically renews the certificates daily at 12:00 AM. The schedule uses the local time zone of the wireless controller.

   Click an available option to select the required schedule.



Note The available options vary based on the number of days entered in the **Due Time** field.

Table 46: Scheduling options

If you want to schedule the certificate renewal...	Then...
daily	select **Daily** and complete these configurations: • Select a start time for certificate renewal. • For the staggered execution, select an end time for certificate renewal.
every week on selected days	select **Weekly** and complete these configurations: • Check the check box next to the days on which you want to schedule the certificate renewal. • Select a start time for certificate renewal. • For the staggered execution, select an end time for certificate renewal.
every month on selected dates	select **Monthly** and complete these configurations: • Check the check box next to the dates on which you want to schedule the certificate renewal. • Select a start time for certificate renewal. • For the staggered execution, select an end time for certificate renewal.

Step 4 Click **Save**.

What to do next

Assign the AP LSC renewal profile to the required wireless controller during provisioning. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 and Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches, on page 668.

Edit an AP LSC renewal profile

Use this procedure to edit an AP Locally Significant Certificate (LSC) renewal profile.

Procedure

Step 1 Navigate to wireless security settings.

a) From the main menu, choose **Design** > **Network Settings**.
b) Click the **Wireless** tab.
c) From the left hierarchy tree, select **Global**.
d) Click **Security Settings**.
e) Click the **AP LSC Certificate Renewal** tab.

Tip If the window displays the **More** drop-down instead of this tab, hover your cursor over **More** and select this tab.

Step 2 Edit an AP LSC renewal profile.

a) Select the AP LSC renewal profile to edit.
b) Click **Edit**.
c) In the **Edit AP LSC Certificate Renewal Profile** slide-in pane, edit the configurations as necessary.

For more information, see Create an AP LSC renewal profile, on page 419.

d) Click **Save**.

Delete AP LSC renewal profiles

Use this procedure to delete one or more AP Locally Significant Certificate (LSC) renewal profiles.

Procedure

Step 1 Navigate to wireless security settings.

a) From the main menu, choose **Design** > **Network Settings**.
b) Click the **Wireless** tab.

c) From the left hierarchy tree, select **Global**.
d) Click **Security Settings**.
e) Click the **AP LSC Certificate Renewal** tab.

Tip If the window displays the **More** drop-down instead of this tab, hover your cursor over **More** and select this tab.

Step 2 Delete one or more AP LSC renewal profiles.

a) Select the AP LSC renewal profiles to delete.
b) Click **Delete**.
c) In the dialog box, click **Delete**.

Create an anchor group

You can create anchor groups with up to 24 Cisco Wireless Controllers and set the priority for the anchors. You can add these devices as anchors:

- Cisco Wireless Controllers that are managed by Catalyst Center.
- Cisco Wireless Controllers that are not managed by Catalyst Center (external wireless controllers).

Note You must add at least one anchor to an anchor group.

The mobility tunnel is established based on the available wireless management IP address present on the paired device. For example, if the active main wireless controller has an IPv6 address and the anchor wireless controller has a wireless management interface configured with dual stack (both IPv4 and IPv6), the mobility tunnel is established using the IPv6 address.

Priority order of the anchors determines the traffic sharing across the anchors:

- Equal sharing: When the priority order of all the anchors is the same (for example, 1, 1, and 1).
- Partial sharing: When the priority order of more than one anchor is the same (for example, 1, 1, and 2).
- Sequential sharing: When the priority order of the anchors is sequential (for example, 1, 2, and 3).

You can associate the anchor group with wireless network profile. For more information, refer to Add SSIDs to a network profile, on page 460.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.
Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Anchor Groups**.

The **Anchor Groups** window opens.

Step 5 In the **Anchor Group** table, click **Add**.

Step 6 In the **Anchor Group Name** field of the **Anchor Group** slide-in pane, enter the anchor group name.

Step 7 To add a managed wireless controller as an anchor, click **Add Managed WLC** and do these steps in the **Add Managed WLC** dialog box:

a) Check the check box for the devices that you want to add as anchors.

To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

Note The wireless controller must have a static IP address assigned to its wireless management interface. It must not be provisioned with the active main role.

b) Click **Add**.

Step 8 (Optional) To add an external wireless controller as an anchor, click **Add External WLC** and do these steps in the **Add External WLC** dialog box:

a) In the **Device Name** field, enter the device name.
b) From the **Device Series** drop-down list, choose a device series.
c) (Optional) In the **Peer IPv4 Address** field, enter the wireless management IPv4 address of the external wireless controller.
d) (Optional) In the **NAT IPv4 Address** field, enter the Network Address Translation (NAT) IPv4 address.
e) (Optional) In the **Peer IPv6 Address** field, enter the wireless management IPv6 address of the external wireless controller.
f) (Optional) In the **NAT IPv6 Address** field, enter the NAT IPv6 address.
g) In the **MAC Address** field, enter the MAC address of the device.
h) In the **Mobility Group Name** field, enter the mobility group name.
i) (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

Note This field is available for only the Cisco Catalyst 9800-CL Wireless Controllers.

j) Click **Add**.

Step 9 (Optional) To add an existing external wireless controller as an anchor, click **Add Existing External WLC** and do these steps in the **Add Existing External WLC** dialog box:

a) Check the check box next to the name of the devices that you want to add as anchors.

To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

b) Click **Add**.

Step 10 (Optional) To set the priority for an anchor, from the **Priority Order** drop-down list, choose the priority for the anchor wireless controller.

Step 11 Click **Save**.

Edit or delete an anchor group

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Anchor Groups**.

Step 5 In the **Anchor Group** table, check the check box next to the anchor group that you want to edit or delete.

- To edit the anchor group, click **Edit**. In the **Anchor Group** slide-in pane, configure the anchors and click **Save**. For more information, see Create an anchor group, on page 422.
- To delete the anchor group, click **Delete** and then click **Yes**.

AP profiles

AP profiles consolidate the AP authentication settings for Plug and Play (PnP), Cisco Advanced Wireless Intrusion Prevention System (aWIPS), rogue management, and mesh networks. AP profiles allow you to manage and provision APs.

Catalyst Center provides a default AP profile for Cisco IOS XE devices and Cisco AireOS devices. You can edit the default AP profiles, but you can't delete them. Site tags and AP groups generated by Catalyst Center use the default AP profiles.

If your authentication method is EAP-Transport Level Security (EAP-TLS), which uses certificate-based authentication, you cannot use a subordinate CA certificate. With EAP-TLS authentication for AP profiles, you can only use a root CA certificate.

Note When you upgrade to Release 2.3.7.x from an earlier version, by default, Catalyst Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the **AP Profiles** window. For more information, see Edit or delete an AP profile, on page 435.

When you save the default AP profile, if there's a difference between the current wireless controller configuration and the AP profile configuration saved on Catalyst Center, Catalyst Center pushes the default AP profile to the wireless controller during subsequent reprovisioning.

After saving the default AP profile, there's no option to prevent Catalyst Center from pushing the default AP profile to the wireless controller during reprovisioning.

You can also create custom AP profiles for Cisco IOS XE and Cisco AireOS devices. To assign an AP profile to a site, associate it with a wireless network profile.

Create an AP profile for Cisco IOS XE devices

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, hover your cursor over **Add** and choose **AP Profile for IOS-XE**.

Step 6 In the **Create Access Point Profile** window, enter a name for the AP profile.

Step 7 (Optional) Enter a description for the AP profile.

Step 8 If this AP profile is for remote teleworker APs or Cisco OfficeExtend APs, check the **Remote Teleworker** check box.

You can enable or disable the **Remote Teleworker** check box only while creating the AP profile. You can't update this option for existing AP profiles.

Note Remote teleworker-enabled AP profiles don't support these settings:

- aWIPS application
- Rogue detection
- Mesh
- Power

Step 9 Configure the required settings in these tabs:

a) **Management**: For more information, see Configure management settings for an AP profile for Cisco IOS XE devices, on page 425.

b) **Security**: For more information, see Configure security settings for an AP profile for Cisco IOS XE devices, on page 428.

c) **Mesh**: For more information, see Configure mesh settings for an AP profile for Cisco IOS XE devices, on page 429.

d) **Power**: For more information, see Configure power settings for an AP profile for Cisco IOS XE devices, on page 430.

e) **Additional**: For more information, see Configure additional settings for an AP profile for Cisco IOS XE devices, on page 431.

Step 10 Click **Save**.

Configure management settings for an AP profile for Cisco IOS XE devices

Use this procedure to configure these settings for an AP profile for Cisco IOS XE devices:

- Authentication settings to onboard APs securely during the PnP claim process. Based on the authentication settings configured at the global-level or site-level hierarchy in Catalyst Center, PnP pushes the 802.1x

(Dot1x) supplicant and certificates when claiming an AP. The AP uses the 802.1x supplicant for authenticating with Cisco ISE.

- Authentication settings for day-*n* authentication of APs.
- Automatic Media Access Control Security (MACsec) configuration for applicable APs.
- Credentials for console access, SSH, and Telnet.
- Enabling Cisco Discovery Protocol (CDP) to make an AP discoverable to its neighboring devices.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Management** tab.

Step 2 In the **Access Points Authentication** area, select an authentication method.

Note This authentication method is used during the AP PnP claim and day-*n* authentication. Changing the authentication method impacts the service of the APs onboarded through the PnP claim process. If you change the authentication method, perform a factory reset for the APs onboarded through PnP claim process. If an AP joins with a different Extensible Authentication Protocol (EAP) method, the EAP method changes based on the authentication method that you select.

These authentication methods are available:

- **NO-AUTH**: Default authentication method.
- **EAP-TLS**: EAP-Transport Level Security (EAP-TLS) uses certificate-based authentication.

  Note EAP-TLS uses the client certificates and server certificates for mutual authentication. To support client certificates on AP, Locally Significant Certificate (LSC) provisioning is supported on APs through day-zero onboarding or PnP claim.

  If the LSC expires, a message is displayed on the AP console every 10 minutes to indicate that the license has expired. However, the AP is allowed to run with an expired certificate until the next reboot. On the subsequent AP reboot, if the LSC has expired, AP deletes its configuration and returns to the day-zero configuration. The PnP discovery process is started again. Catalyst Center displays the reboot reason as DOT1X_LSC_EXPIRY.

  To renew the LSC on day-*n* before it expires, use the **capwap ap erase lsc-cert** command on APs running Cisco IOS XE Release 17.9.6 and later.

- **EAP-PEAP**: EAP-Protected Extensible Authentication Protocol (EAP-PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. EAP-PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol.

If you select **EAP-PEAP**, enter a username and password. Catalyst Center generates a certificate and applies it during the PnP claim process.

- **EAP-FAST**: EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

  If you select **EAP-FAST**, enter a username and password. Catalyst Center generates a certificate and applies it during the PnP claim process.

Step 3 If you choose the **EAP-TLS** or **EAP-FAST** authentication method, use the **MACsec Encrypted** toggle button to enable or disable MACsec encryption of AP uplink traffic using 802.1x.

Note Before you enable MACsec encryption for AP uplink traffic, ensure that the Cisco ISE AP onboarding authorization profile returns the required MACsec attributes to the access switch. For more information, refer to Configure Cisco ISE for fabric AP MACsec on edge nodes, on page 1049.

This option is applicable for:

- Cisco Catalyst 9000 Series Switches running Cisco IOS XE Release 26.1.1 or later.
- Wireless controllers running Cisco IOS XE Release 26.1.1 or later.

For information about applicable APs, refer to Feature Matrix for Cisco Wireless Access Points.

Catalyst Center does not support MACsec encryption for fabric sites that contain a Cisco Catalyst 9350 Series Smart Switch.

If you enable MACsec encryption, in the **Replay Protection Window Size** field, enter a number to specify the size of the replay protection window for MACsec. The default value is 0, indicating that out-of-order packets are not allowed.

Step 4 In the **Auto-Secure MACsec Configuration** area, use the **Auto-Secure MACsec** toggle button to enable or disable automatic MACsec configuration on supported APs.

This configuration is supported only on Wi-Fi 7 APs and Cisco Catalyst 9350 Series Smart Switches running Cisco IOS XE Release 26.2.1 or later. For information about applicable APs, refer to Feature Matrix for Cisco Wireless Access Points.

Note This configuration is supported only in nonfabric deployments on Cisco Catalyst 9350 Series Smart Switches. It is not supported in fabric deployments.

Step 5 In the **SSH and Telnet** area, do this configuration:

a) (Optional) Click the **SSH** toggle button to configure the credentials for SSH.
b) (Optional) Click the **Telnet** toggle button to configure the credentials for Telnet.
c) In the **Username** field, enter the name used to authenticate the device.

   The username can’t contain spaces or angle brackets (< >).

Note If you disable SSH and Telnet, the **Username** field is optional.

d) In the **Password** field, enter the password used to authenticate the device.

Note If you disable SSH and Telnet, the **Password** field is optional.

e) In the **Enable Password** field, enter the password to enable a higher privilege level in the CLI.

Note If you disable SSH and Telnet, the **Enable Password** field is optional.

Step 6 In the **Cisco Discovery Protocol (CDP) State** area, click the **CDP State** toggle button to enable or disable CDP.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP profile for Cisco IOS XE devices, on page 425.

Configure security settings for an AP profile for Cisco IOS XE devices

Use this procedure to configure these security settings for an AP profile for Cisco IOS XE devices:

- Cisco Advanced Wireless Intrusion Prevention System (aWIPS) and forensic capture to detect intrusion threats and mitigate them. Catalyst Center supports aWIPS for devices running Cisco IOS XE Release 17.3.1 or later.
- Rogue detection to detect the APs that are installed on the network without explicit authorization from a system administrator. Catalyst Center supports rogue detection for devices running Cisco IOS XE Release 17.4 or later.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Security** tab.

Step 2 In the **aWIPS and Forensic Capture Enablement** area, do this configuration:

a) Click the **aWIPS** toggle button to enable or disable aWIPS.

b) Click the **Forensic Capture Enablement** toggle button to enable or disable forensic capture.

Note You must enable the **aWIPS** toggle button to use the **Forensic Capture Enablement** toggle button.

Step 3 In the **Rogue Detection** area, do this configuration:

a) Click the **Rogue Detection** toggle button to enable or disable rogue detection.

b) In the **Minimum RSSI** field, enter the valid RSSI value. The valid range is from -128 to -70 dBm. The default value is -90 dBm.

c) In the **Transient Interval** field, enter a valid transient time interval in seconds. The valid transient interval ranges from 120 to 1800 seconds. The default value is 0.

d) In the **Report Interval** field, enter a valid report time interval in seconds. The valid report interval ranges from 10 to 300 seconds. The default value is 10 seconds.

Step 4 In the **Rogue Containment** area, click the **PMF Denial** toggle button to enable the containment for rogue AP doing Protected Management Frame (PMF).

Note **PMF Denial** is supported from IOS-XE version 17.12 and above.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP profile for Cisco IOS XE devices, on page 425.

Configure mesh settings for an AP profile for Cisco IOS XE devices

Use this procedure to configure the mesh settings for an AP profile for Cisco IOS XE devices.

Before you begin

Ensure that you add the MAC address of the mesh access point (MAP) to the AP authorization list. For more information, see Create an AP authorization list, on page 417.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Mesh** tab.

Step 2 Click the **Mesh** toggle button.

Note If you disable the **Mesh** toggle button, the existing custom mesh settings are deleted, and the AP profile is associated with the default mesh profile on the device.

Step 3 (Optional) In the **Range - Root AP to Mesh AP (in feet)** field, enter the maximum range (in feet) from the root access points (RAP) to the MAPs in the network. The valid range is from 150 feet through 132000 feet.

Step 4 (Optional) To allow wireless client association over the backhaul radio, check the **Backhaul Client Access** check box.

Generally, the backhaul radio is a 5-GHz radio for most of the MAPs. The backhaul radio can carry both backhaul traffic and client traffic.

If you disable the **Backhaul Client Access** check box, Catalyst Center sends only backhaul traffic over the backhaul radio, and client association is only over the secondary radio or radios.

Step 5 (Optional) In the **RAP Downlink Backhaul** area, choose the required option.

If your country prohibits the use of **5 GHz**, choose **2.4 GHz**. Even if your country allows the use of **5 GHz**, consider using **2.4 GHz** because 2.4-GHz radio can cover larger mesh or bridge distances.

Note

- For a mesh AP, when you change the mesh role to RAP and provision the AP, the AP reboots. RAP downlink backhaul mesh settings are effective only after the reboot.
- When you change the RAP configuration from **5 GHz** to **2.4 GHz**, Catalyst Center propagates the update from the RAP to all the MAPs. At this point, the MAPs disconnect from the 5-GHz network and connect to the 2.4-GHz network.

Step 6 (Optional) In the **Backhaul Data Rates** area, from the **5GHz Band Radio Type** and **2.4GHz Band Radio Type** drop-down lists, choose an interface rate.

Valid backhaul interface rates are **802.11abg**, **802.11n**, **802.11ac** (5-GHz band radio only), **802.11ax**, and **Auto**, depending on the AP. Backhaul creates a wireless connection between the APs. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices.

With the **Auto** data rate, each link can arrive at the best possible rate for its link quality.

We recommend that you configure the mesh backhaul data rate as **Auto**.

Step 7 (Optional) In the **Bridge Group Name** field in the **Bridge Group** area, enter a name of up to 10 characters for the bridge group.

A bridge group name controls the association of MAPs. By grouping radios, two networks on the same channel, but in different bridge group names can’t communicate with one another. This setting is also useful if you have more than one RAP in your network in the same sector (area).

If you don't enter a bridge group name, Catalyst Center uses the **Default** bridge group name for the mesh profile.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP profile for Cisco IOS XE devices, on page 425.

Configure power settings for an AP profile for Cisco IOS XE devices

Use this procedure to configure these power settings for an AP profile for Cisco IOS XE devices:

- AP power profile: If an AP doesn't receive the required power, it functions in a derated state based on the settings in the AP power profile. For more information, see Create an AP power profile, on page 436.

Note The power settings are applicable only for the Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later.

- Calendar power profile: You can create calendar power profiles for APs that are in power save mode. You can map multiple AP power profiles to different calendar schedules as required. Based on the configured schedule, Catalyst Center runs all the rules defined in the AP power profiles simultaneously.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Power** tab.

Step 2 In the **AP Power Profile** area, from the **Select Value** drop-down list, choose a power profile.

(To create a power profile, click **Create New** and configure the parameters. For more information, see Create an AP power profile, on page 436.)

Step 3 In the **Calendar Power Profile** area, do these steps:

a) To add a calendar power profile, click **Add**. In the **Add Calendar Power Profile** slide-in pane, do these steps:

1. From the **Select Power Profile** drop-down list, choose a power profile.

   To create a power profile, click **Create New** and configure the parameters. For more information, see Create an AP power profile, on page 436.

2. Choose the recurrence frequency for applying the power profile rules to the APs:
   - **Daily**: Applies the power profile rules to APs daily.
   - **Weekly**: Applies the power profile rules to APs every week on the selected days. Click the required day to select it.
   - **Monthly**: Applies the power profile rules to APs every month on the selected dates. Click the required date to select it.
3. Specify the start time and end time for the power profile rules.
4. Click **Save**.

b) (Optional) To edit a power profile rule, check the check box next to the corresponding power profile name and click **Edit**. In the **Edit Power Profile** slide-in pane, edit the required parameters and click **Save**.

c) (Optional) To delete a power profile, check the check box next to the corresponding power profile name, click **Delete**, and then click **Yes**.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP profile for Cisco IOS XE devices, on page 425.

Configure additional settings for an AP profile for Cisco IOS XE devices

Use this procedure to configure these additional settings for an AP profile for Cisco IOS XE devices:

- Country code: Set the country code for the Rest of World (ROW) domain APs that don't have a country code configured already.

Note The country code setting doesn't impact the APs that already have a country code configured.

- Time zone: Choose the time zone for the APs.
- Client limit: Specify the maximum number of allowed clients.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for IOS-XE**), click the **Additional** tab.

Step 2 In the **Country Code** area, from the **Select Value** drop-down list, choose a country for ROW APs that don't have a country code configured.

Step 3 In the **Time Zone** area, choose one of these options:

- **Not Configured**: APs operate in the UTC time zone.
- **Controller**: APs operate in the Cisco Wireless Controller time zone.
- **Delta from Controller**: APs operate in the offset time from the wireless controller time zone. Configure these offset values:
  - **HH**: Enter the hour value. The valid range is from -12 through 14.
  - **MM**: Enter the minute value. The valid range is from 0 through 59.

Step 4 In the **Client Limit** area, enter a value for the maximum client limit. The valid range is from 0 through 1200.

What to do next

After configuring all the necessary settings for the AP profile, click **Save**. For more information, see Create an AP profile for Cisco IOS XE devices, on page 425.

Create an AP profile for Cisco AireOS devices

For Cisco AireOS devices, AP profiles group the AP-level parameters and configurations. AP profiles can be mapped to custom AP groups. When APs are provisioned, all APs under the corresponding AP group are configured with the settings available in the AP profile.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, hover your cursor over **Add** and choose **AP Profile for AireOS**.

Step 6 In the **Create Access Point Profile** window, enter a name for the AP profile.

Step 7 (Optional) Enter a description for the AP profile.

Step 8 If this AP profile is for remote teleworker APs or Cisco OfficeExtend APs, check the **Remote Teleworker** check box.

You can enable or disable the **Remote Teleworker** check box only while creating the AP profile. You can't update this option for existing AP profiles.

Note Remote teleworker-enabled AP profiles don't support these settings:

- Rogue detection
- Mesh

Step 9 Configure the required settings in these tabs:

a) **Management**: For more information, see Configure management settings for an AP profile for Cisco AireOS devices, on page 433.

b) **Security**: For more information, see Configure security settings for an AP profile for Cisco AireOS devices, on page 434.

c) **Mesh**: For more information, see Configure mesh settings for an AP profile for Cisco AireOS devices, on page 434.

Step 10 Click **Save**.

Configure management settings for an AP profile for Cisco AireOS devices

Use this procedure to configure these settings for an AP profile for Cisco AireOS devices:

- Credentials for console access, SSH, and Telnet.
- Enable Cisco Discovery Protocol (CDP) to make the AP discoverable to its neighboring devices.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for AireOS**), click the **Management** tab.

Step 2 In the **SSH and Telnet** area, do this configuration:

a) (Optional) Click the **SSH** toggle button to configure the credentials for SSH.

b) (Optional) Click the **Telnet** toggle button to configure the credentials for Telnet.

c) In the **Username** field, enter the name used to authenticate the device.

Username can’t contain spaces or angle brackets (< >).

Note If you disable SSH and Telnet, the **Username** field is optional.

d) In the **Password** field, enter the password used to authenticate the device.

Note If you disable SSH and Telnet, the **Password** field is optional.

e) In the **Enable Password** field, enter the password to enable a higher privilege level in the CLI.

Note If you disable SSH and Telnet, the **Enable Password** field is optional.

Step 3 In the **Cisco Discovery Protocol (CDP) State** area, click the **CDP State** toggle button to enable or disable CDP.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP profile for Cisco AireOS devices, on page 432.

Configure security settings for an AP profile for Cisco AireOS devices

Use this procedure to configure rogue detection for an AP profile for Cisco AireOS devices. Rogue detection allows you to detect the APs that are installed on the network without explicit authorization from a system administrator.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for AireOS**), click the **Security** tab.

Step 2 In the **Rogue Detection** area, click the **Rogue Detection** toggle button to enable or disable rogue detection.

What to do next

Configure the other necessary settings for the AP profile. For more information, see Create an AP profile for Cisco AireOS devices, on page 432.

Configure mesh settings for an AP profile for Cisco AireOS devices

Use this procedure to configure the mesh settings for an AP profile for Cisco AireOS devices.

Before you begin

Ensure that you add the MAC address of the MAP to the AP authorization list. For more information, see Create an AP authorization list, on page 417.

Procedure

Step 1 In the **Create Access Point Profile** window (**Design** > **Network Settings** > **Wireless** > **AP Profiles** > **Add** > **AP Profile for AireOS**), click the **Mesh** tab.

Step 2 Click the **Mesh** toggle button.

Step 3 (Optional) In the **RAP Downlink Backhaul** area, click the radio button next to the required option.

If your country prohibits the use of **5 GHz**, choose **2.4 GHz**. Even if your country allows the use of **5 GHz**, consider using **2.4 GHz** because 2.4-GHz radio can cover larger mesh or bridge distances.

Note

- For a mesh AP, when you change the mesh role to RAP and provision the AP, the AP reboots. RAP downlink backhaul mesh settings are effective only after the reboot.
- When you change the RAP configuration from **5 GHz** to **2.4 GHz**, Catalyst Center propagates the update from the RAP to all the MAPs. At this point, the MAPs disconnect from the 5-GHz network and connect to the 2.4-GHz network.

Step 4 (Optional) In the **Bridge Group Name** field in the **Bridge Group** area, enter a name of up to 10 characters for the bridge group.

A bridge group name controls the association of MAPs. By grouping radios, two networks on the same channel, but in different bridge group names, can't communicate with one another. This setting is also useful if you have more than one RAP in your network in the same sector (area).

If you don't enter a bridge group name, Catalyst Center uses the **Default** bridge group name for the mesh profile.

What to do next

After configuring all the necessary settings for the AP profile, click **Save**. For more information, see Create an AP profile for Cisco AireOS devices, on page 432.

Edit or delete an AP profile

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **AP Profiles**.

Step 5 In the **AP Profile** table, check the check box next to the AP profile that you want to edit or delete.

- To edit the AP profile, click **Edit**. In the **Edit Access Point Profile** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see Create an AP profile for Cisco AireOS devices, on page 432 and Create an AP profile for Cisco IOS XE devices, on page 425.
- To delete the AP profile, click **Delete**, and then click **Yes**.

Create an AP power profile

You can create AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. Assign an AP power profile to APs by associating it to an AP profile. You can define multiple rules for an AP power profile and specify the sequences of rules.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Power Profile**.

Step 5 In the **AP Power Profile** table, click **Add**.

Step 6 In the **Power Profile Name** field of the **Create Power Profile** slide-in pane, enter a name for the AP power profile.

Step 7 (Optional) In the **Description** field, enter a description for the AP power profile.

Step 8 Click **Add** to create a rule for the AP power profile.

Step 9 In the **Rule** dialog box, do this configuration:

a) From the **Interface** drop-down list, choose a type of interface.

b) From the **Interface ID** drop-down list, choose an interface ID.

Note If only one interface ID is available, Catalyst Center automatically selects the available interface ID.

c) From the **Parameter** drop-down list, choose a parameter.

Note If only one parameter is available, Catalyst Center automatically selects the available parameter.

d) From the **Parameter Value** drop-down list, choose a parameter value.

Note If only one parameter value is available, Catalyst Center automatically selects the available parameter value.

e) Click **Add**.

Step 10 (Optional) To create another rule for the AP power profile, repeat Step 8, on page 436 and Step 9, on page 436.

Step 11 (Optional) To update the sequence of a rule in the **Rules** table, click the corresponding icon, and drag and drop the rule to the required position.

Step 12 Click **Save**.

What to do next

Associate the AP power profile with an AP profile. For more information, see Create an AP profile for Cisco IOS XE devices, on page 425.

Edit or delete an AP power profile

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Power Profile**.

Step 5 In the **AP Power Profile** table, check the check box next to the AP power profile that you want to edit or delete.

- To edit the AP power profile, click **Edit**. In the **Edit Power Profile** slide-in pane, edit the description, rules, and sequence as necessary, and click **Save**. For more information, see Create an AP power profile, on page 436.
- To delete the AP power profile, click **Delete**, and then click **Yes**.

Provision a Cisco sensor SSID for nonfabric deployment

- The Cisco sensor provisioning Service Set Identifier (SSID) communicates with the Plug and Play (PnP) server to obtain day-zero configurations for running tests.

Note The Cisco sensor provisioning SSID isn't applicable for APs working as sensors.

- For fabric deployments, the Cisco sensor provisioning SSID is mapped to an Infrastructure Virtual Network Access Point (INFRA VN–AP) pool to communicate with Catalyst Center.
- These platforms support the Cisco sensor provisioning SSID:
  - Cisco AireOS Wireless Controller
  - Cisco Catalyst 9800 Series Wireless Controller (both fabric and nonfabric deployments)
- The Cisco sensor provisioning SSID supports these network controllers:
  - Cisco Catalyst 9800 Series Wireless Controllers for Cloud

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco AireOS Wireless Controller

This procedure enables you to configure the Cisco sensor provisioning SSID for nonfabric deployments.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 Click **SSIDs**.

Step 4 From the **SSID** table, hover over Add and choose **Enterprise**.

The **Wireless SSID** workflow opens.

Step 5 In the **Basic Settings** window, click the **Sensor** field and then click **Next**.

Note The parameters for the SSID are automatically populated and can't be edited.

Step 6 In the **Associate SSID to Profile** window, from the left pane, select a profile and do these steps:

a) Under **Fabric**, select **Yes**.
b) Click **Associate Profile**.
c) Click **Next**.

Note If you don't have a profile, click **Add Profile** and configure the profile settings.

Step 7 In the **Summary** window, review the configuration settings.

Step 8 Click **Save**.

Step 9 From the main menu, choose **Provision** > **Inventory**.

Step 10 Check the check box next to a device and from the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 11 Review the details under **Assign Site**, **Configuration**, **Feature Templates**, **Advanced Configuration**, and **Summary**. Click **Next** after each screen.

Step 12 Click **Deploy**.

The **Provision Device** dialog box is displayed.

Step 13 Choose **Now** and click **Apply**.

Result: The message **Task Scheduled view status in Tasks** is displayed at the bottom-right corner.

Step 14 (Optional) After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

Manage backhaul settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Catalyst Center.

Procedure

Step 1 From the main menu, choose **Assurance** > **Settings** > **Sensors**.

The **Sensor List** window appears.

Step 2 Hover your cursor over the **Settings** tab and select **Backhaul Settings**.

Step 3 You can add and manage backhaul SSIDs by doing these steps:

a) Click **+ Add Backhaul**.

The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

b) In the **Settings Name** field, enter a name for the backhaul SSID.

c) In the **Wired Backhaul** area, do this configuration:

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
  - **802.1x EAP**: Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.
  - **Open**: No security or authentication is used.
- **EAP Method**: If you select **802.1x EAP**, you must select one of these EAP methods for user authentication from the drop-down list:
  - **EAP-FAST**: Enter the username and password in the fields provided.
  - **PEAP-MSCHAPv2**: Enter the username and password in the fields provided.
  - **EAP-TLS**: Select **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you select **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.
  - **PEAP-TLS**: Select **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you select **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and do this configuration.

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
  - **WPA2 Enterprise**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.
  - **WPA2-Personal**: Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.

- **PSK Format**: The available preshared key formats are:
  - **ASCII**: Supports ASCII PSK passphrase.
  - **HEX**: Supports 64-character HEX key PSK password.
- **Open**: No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing these steps:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and select **Edit**.

Step 5 You can delete a backhaul configuration by doing these steps:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and select **Delete**.

Create an antenna radio profile

Catalyst Center supports the C-ANT9104 antenna, which integrates with the Cisco Catalyst 9130AXE Unified Access Point to provide dual 5-GHz 4x4 radios with high gain, steerable, and switchable functions. With Catalyst Center, you can select the beam steering (direction) for the antennae. Available modes include:

- Wide beam
- Narrow beam
- Narrow beam with 10 degrees of tilt
- Narrow beam with 20 degrees of tilt

You can configure wide and narrow beamwidth states for installations where high user density, precise pattern control, and long-range performance in the 5-GHz band are required.

The beam steering configuration is available for antenna combinations ABCD (left antennae) and EFGH (right antennae). The antenna pattern names are set based on the selected beam. You can visualize the heatmaps on Catalyst Center floor maps.

You can use the antenna radio profile during AP provisioning. For more information, see Provision Cisco APs on day 1, on page 627.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Antenna Radio Profiles**.

Step 5 In the **Antenna Radio Profile** table, click **Add**.

Step 6 Configure wide and narrow beam steering for the antennae in the **Antenna Radio Profile** slide-in pane:

- In the **Radio Profile Name** field, enter a unique name for the radio profile.
- From the **Beam Steer Mode** drop-down list, choose a beam steering mode.

Step 7 Click **Save**.

The new antenna radio profile displays in the **Antenna Radio Profile** table.

Edit or delete an antenna radio profile

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **Antenna Radio Profiles**.

Step 5 In the **Antenna Radio Profile** table, check the check box next to the antenna radio profile name that you want to edit or delete.

- To edit the antenna radio profile, click **Edit**. In the **Antenna Radio Profile** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see Create an antenna radio profile, on page 440.
- To delete the antenna radio profile, click **Delete** and then click **Yes**.

Cisco Connected Mobile Experiences integrations

A Cisco Connected Mobile Experiences integration is a wireless mapping feature that

- enables the integration of on-premises Cisco Connected Mobile Experiences (CMX) for enhanced location tracking,
- displays the precise location of wireless clients, rogue access points, and interferers within the user interface, and
- supports customizable CMX settings that adapt to enterprise size, from global to site or floor level.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level, and for a large enterprise, you can assign CMX at the floor level.



Note CMX should be anonymized for security purposes.

Create Cisco CMX settings

Before you begin

Ensure that CMX is configured with a valid SSL/TLS certificate. See the CMX 10.5 SSL certificate installation procedure.

Procedure

Step 1 From the main menu, choose **System** > **Settings**.

Step 2 From the **External Services** section, click **Cisco Spaces/CMX Servers**.

The **Cisco Spaces/CMX Servers** window opens.

Step 3 From the **CMX Servers** table, click **Add**.

Step 4 Complete the fields in the **Add CMX Server** slide-in pane:

- **IP Address**: Enter the valid IP address of the CMX web GUI.
- **Username**: Enter the CMX web GUI admin username.

Note To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**. For more information, see "Catalyst Center user role permissions" in the *Cisco Catalyst Center Administrator Guide*.

- **Password**: Enter the password credentials.

Note Ensure CMX is reachable.

Step 5 Click **Add**.

The connection status is shown in these stages:

- **Initiating Connection**: Verifies connectivity to the server.
- **Establishing Trust**: Establishes trust to the CMX server. The CMX server must have a valid SSL/TLS certificate configured to establish trust. If the certificate is not yet stored in Catalyst Center Trusted Certificates, you are prompted to **Accept** the certificate to continue.
- **Connecting CMX Server**: Validates the user credentials provided.

Step 6 To assign a CMX server to a site, building, or a floor, click the menu icon and choose **Design** > **Network Settings**.

Step 7 Click the **Wireless** tab.

Step 8 From the left hierarchy tree, select either **Global** or the required area, building, or floor.

Step 9 Click **Cisco Spaces/CMX Servers**.

Step 10 In the **Cisco Spaces/CMX Servers** section, from the **Location Settings** drop-down list, select the CMX server.

Step 11 Click **Save**.

The **Create CMX Settings** window opens.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Catalyst Center starts querying the CMX for the client location and displays the location on the floor map.

Step 12 From the floor map, you can do these tasks:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box appears with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.
- Click an AP to open a side bar with details about the AP.
- Do real-time client tracking when Intelligent Capture and CMX are integrated.

Step 13 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** window, hover your cursor over the ellipsis ••• next to the building or floor on which you made the changes in the left hierarchy tree, and then select **Sync: Cisco Spaces/CMX Servers** to push the changes manually.

Step 14 To edit the CMX server details or delete a CMX server:

a) From the main menu, choose **System** > **Settings**.
b) From the **External Services** section, click **Cisco Spaces/CMX Servers**.
c) Select the CMX server that you want to edit, make any changes, and click **Update**.
d) Select the CMX server that you want to delete and click **Delete**.
e) Click **OK** to confirm the deletion.

For CMX connection failure

- Check if you have uploaded the CMX certificate to **System** > **Settings** > **Trusted Certificates**.
- After upgrading to Catalyst Center, edit the CMX connection details to reestablish the connection by reviewing and accepting the CMX SSL/TLS certificate.

For CMX authentication failure

- Check if you are able to log in to the CMX web GUI with the credentials that you provided at the time of CMX settings creation on Catalyst Center.
- Check if you are able to log in to the CMX console using SSH.
- Check if you are able to exercise CMX REST APIs using the API documentation link on the CMX GUI.

If clients do not appear on the Catalyst Center floor map

- Check if the Cisco Wireless Controller on the particular floor is configured with CMX and is active.
- Check if the CMX GUI shows clients on the floor map.
- Choose **Data/Filters** > **Clients** and click the **Unpositioned** tab to check why clients aren't appearing on the floor map.

About Cisco Spaces integration

Enterprises operating in the physical world have limited to no visibility into the behavior of people and connected assets within their buildings. Cisco Spaces solves this physical blind-spot problem using location-sensing intelligence from all underlying Cisco wireless networks and translating the data into business-ready insights.

Catalyst Center integrates with Cisco Spaces to provide you with the exact location of wireless clients, rogue APs, and interferers on Catalyst Center floor maps. Depending on your requirements, you can create Cisco Spaces settings either at the global level or at the site, building, or floor level.

After a Cisco Spaces/CMX sync is triggered, you can view the sync status by clicking the floor map and choosing **More** > **CMX/Cisco Spaces Sync History**.

To integrate Cisco Spaces with Catalyst Center, see the "Catalyst Center Integration" section in the *Cisco Spaces Configuration Guide*.

Assign Cisco Spaces to sites

To monitor sites using Cisco Spaces, you need to assign Cisco Spaces to the site that you want to monitor.

Before you begin

Integrate Cisco Spaces with Catalyst Center. For details, see the *Cisco Spaces Configuration Guide*.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select either **Global** or the area, building, or floor to which you want to assign Cisco Spaces.

Step 4 Click **Cisco Spaces/CMX Servers**.

Step 5 In the **Cisco Spaces/CMX Servers** window, from the **Location Services** drop-down list, select a site.

Step 6 Click **Save**.

Catalyst Center deploys the site information to Cisco Spaces automatically.

Monitor sites using Cisco Spaces

You can monitor sites using Cisco Spaces.

Before you begin

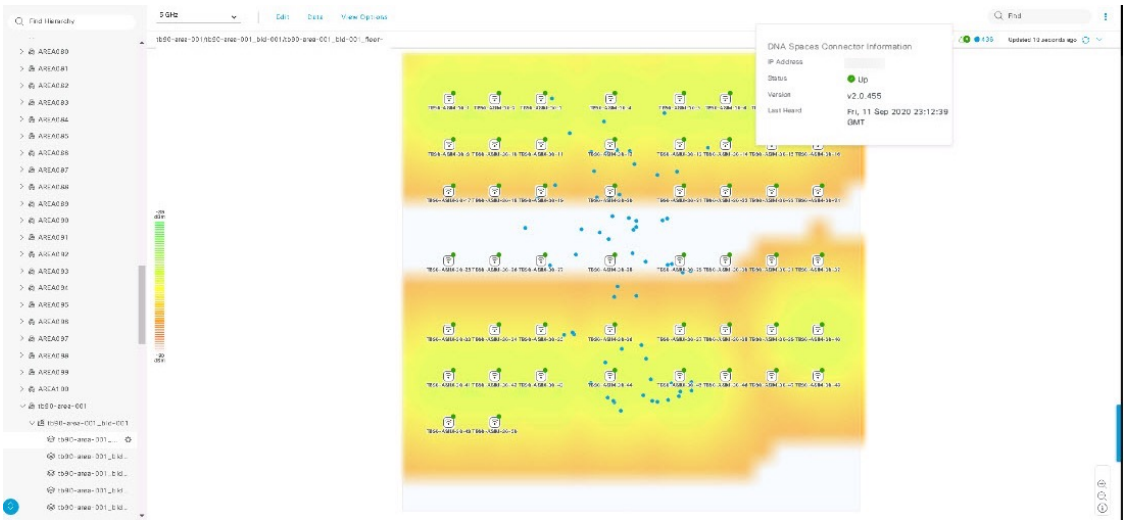
- Integrate Cisco Spaces with Catalyst Center. For details, see the *Cisco Spaces Configuration Guide*.
- Assign Cisco Spaces to the site that you want to monitor.

Procedure

Step 1 In the Catalyst Center GUI, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, select either **Global** or the area, building, or floor that you want Cisco Spaces to monitor.

Step 3 To confirm that Cisco Spaces is operational, verify that the Cisco Spaces/CMX status icon displays on the floor that you want to monitor, as shown in this figure.



Configure a FlexConnect VLAN

You can configure FlexConnect VLAN settings, including:

- **Native VLAN**: Allows a FlexConnect group to carry the management traffic between APs and Cisco Wireless Controllers.
- **AAA Override VLAN**: Provides dynamic VLAN assignment of locally switched clients.

You can apply these settings at the global level and override them at the site, building, or floor level.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select the required site:

- **Global**: Configures the VLAN at the global level for all sites.
- Area, building, or floor: Configures the VLAN at the chosen level only.

Step 4 Click **FlexConnect Settings**.

Child sites inherit the FlexConnect settings from the parent site. Inherited settings are displayed with an inherit icon next to the setting; hover your cursor over the icon to see the origin of the setting. You can use the **Delete** option to delete a setting and the **Inherit** option to inherit settings from the parent site, if it hasn't been inherited.

Step 5 In the **Native VLAN ID** field, enter a value for the VLAN ID. The valid range is from 1 through 4094.

Step 6 For the **AAA Override VLAN** settings, enter a VLAN ID and VLAN name mapping in the corresponding **VLAN ID** and **VLAN Name** fields. To add more mappings, click the **Add** icon.

Note The maximum number of VLAN mappings that you can define for a FlexConnect deployment is 16. However, for Cisco Catalyst 9800 Series Wireless Controllers, this number includes default WLAN VLANs and VLANs pushed by AAA.

Step 7 Click **Save**.

What to do next

Create a wireless network profile *or* configure an SSID:

- **Wireless Network Profile**: If you decide to create a wireless network profile, make sure that the **FlexConnect Local Switching** check box is checked. For more information, see Create network profiles for wireless, on page 460.
- **SSID**: If you want to configure an SSID, see Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

For the saved FlexConnect VLAN settings to get configured on the wireless controller, you must provision the wireless controller. For information, see Provision a Cisco AireOS Controller, on page 620 or Configure and provision a Cisco Catalyst 9800 Series Wireless Controller, on page 634.

After provisioning the wireless controller, you must provision the AP that is associated with the controller.

Create an 802.11be profile

The 802.11be profile enables Wi-Fi 7 configuration on wireless controllers that are running Cisco IOS XE Release 17.15.2 or later.

With this profile, you can configure Multi-Link Operation (MLO) groups to use multiple frequency bands simultaneously. This configuration improves overall wireless performance.

Note

- This 802.11be profile is mapped to the WLAN and applies only to the 2.4-GHz and 5-GHz bands. For the 6-GHz band, the 802.11be configuration uses the corresponding settings from the RF profile. For more information, see Create a wireless radio frequency profile, on page 383 and Create an AI radio frequency profile, on page 396.
- Wireless controllers that are running versions earlier than Cisco IOS XE Release 17.18.1 use only a single dot11be-profile, which is the default-dot11be-profile. Use only one 802.11be profile across SSIDs and network profiles for each wireless controller.
- Wireless controllers that are running Cisco IOS XE Release 17.18.1 or later support custom 802.11be profiles. You can use multiple 802.11be profiles across SSIDs in a network profile for a wireless controller.

  For information about associating an 802.11be profile with a wireless network profile, see Add SSIDs to a network profile, on page 460.
- The MLO group configurations are supported on wireless controllers that are running Cisco IOS XE Release 17.18.1 or later

Before you begin

Enable the global 802.11be status in the **Dot11be Status Configuration** feature template. Then provision the managing wireless controller to apply 802.11be profile configurations.

For more information about enabling 802.11be status in the feature template, see Create a feature template for Dot 11be status configuration, on page 521. For information about provisioning the wireless controller, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **802.11be Profiles**.

Step 5 In the **802.11be Profiles** table, click **Add**.

Step 6 In the **802.11be Profile Name** field of the **Add 802.11be Profile** slide-in pane, enter the 802.11be profile name.

Step 7 Enable the **Mark as default** toggle button to set this profile as the default profile.

Marking this profile as the default profile pushes the configuration to the default-dot11be-profile on the wireless controller.

Note This configuration is supported only on the wireless controllers that are running Cisco IOS XE Release 17.18.1 or later.

Step 8 In the **Description** field, enter a description.

Step 9 (Optional) Use the toggle buttons to enable or disable these configurations:

- **OFDMA Uplink**: Enables uplink connection to use OFDMA.
- **OFDMA Downlink**: Enables downlink connection to use OFDMA.
- **MU-MIMO Uplink**: Enables uplink connection to use MU-MIMO.
- **MU-MIMO Downlink**: Enables downlink connection to use MU-MIMO.
- **OFDMA Multi-RU**: Enables the assignment of multiple Resource Units (RUs) simultaneously to a single user using OFDMA.



Note Starting in Cisco IOS XE Release 17.18.2, the **OFDMA Uplink**, **OFDMA Downlink**, **MU-MIMO Uplink**, and **MU-MIMO Downlink** configurations are deprecated and ignored in the 802.11be profile. To configure these settings, use the **802.11ax Configuration** tab in the **Advanced SSID Configuration** feature template. For more information, see Create a feature template for advanced SSID, on page 512.

Step 10 Use the toggle buttons to enable or disable these MLO group configurations:

- **Primary 2.4GHz**: Configures the 2.4-GHz band in the MLO group
- **Primary 5GHz**: Configures the 5-GHz band in the MLO group
- **Secondary 5GHz**: Configures a secondary 5-GHz band in the MLO group
- **Primary 6GHz**: Configures the 6-GHz band in the MLO group

Step 11 Click **Save**.

Edit or clone an 802.11be profile

Use this procedure to edit or clone an 802.11be profile.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **802.11be Profiles**.

Step 5 In the **802.11be Profiles**, check the check box next to the 802.11be profile that you want to edit or clone.

Step 6 To edit the profile, click **Edit**.

a) In the **Edit 802.11be Profile** slide-in pane, edit the parameters as necessary.

For more information, see Create an 802.11be profile, on page 446.

b) Click **Save**.

Step 7 To clone the profile, click **Clone**.

a) In the **802.11be Profile Name** field of the **Clone 802.11be Profile** slide-in pane, update the 802.11be profile name and edit the other parameters as necessary.

For more information, see Create an 802.11be profile, on page 446.

b) Click **Save**.

Delete 802.11be profiles

Use this procedure to delete 802.11be profiles.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, select **Global**.

Step 4 Click **802.11be Profiles**.

Step 5 In the **802.11be Profiles**, check the check box next to the 802.11be profiles that you want to delete.

Step 6 Click **Delete**.

Step 7 In the dialog box, click **Yes**.

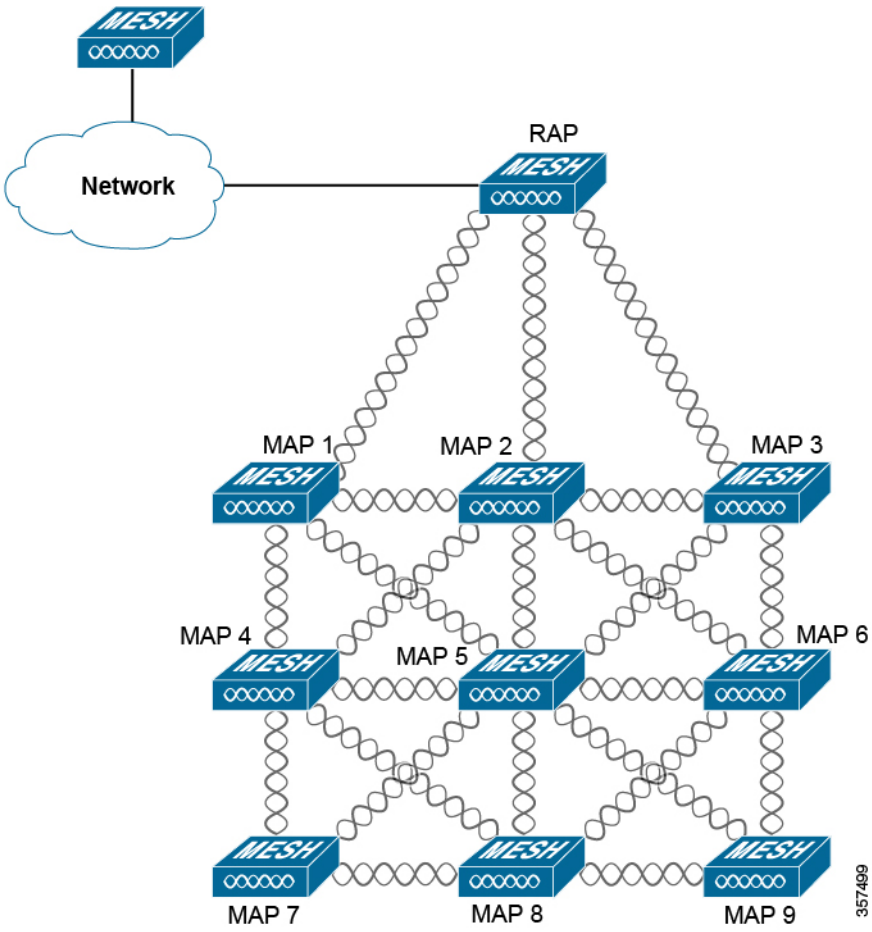
About wireless mesh networks

In a Cisco wireless mesh network, Access Points (APs) operate in one of these two ways:

- Root Access Point (RAP): Connected to the wired network at each location.
- Mesh Access Point (MAP): Communicate wirelessly while providing a secure and scalable wireless LAN.

Note All APs are configured and shipped as MAPs. To use an AP as a RAP, you must reconfigure it as a RAP. In all mesh networks, make sure that there is at least one RAP.

RAPs are connected to the wired network at each location. All the downstream APs operate as MAPs and communicate using wireless links.



Both MAPs and RAPs can provide WLAN client access. However, typically, the location of RAPs is often not suitable for providing client access.

Some buildings have onsite controllers to end Control and Provisioning of Wireless Access Point (CAPWAP) sessions from the MAPs, but it's not a mandatory requirement because CAPWAP sessions can be backhauled to a wireless controller over a WAN.

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. This traffic can come from wired devices that are being bridged by the wireless mesh or CAPWAP traffic from the MAPs. This traffic is always AES encrypted when it crosses a wireless mesh link, such as a wireless backhaul.

For more information about mesh networks, see the latest *Cisco Wireless Mesh Access Points, Design and Deployment Guide*.

Cisco Wireless Controller configuration

For mesh networks, you must configure a list of authorized APs in the wireless controller. Wireless controllers respond only to requests from the MAPs that are present in its authorization list.

Note Catalyst Center supports the configuration of authorization lists on Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS Release 17.5 and later.

Both Cisco AireOS Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller can use Catalyst Center to configure the Bridge Group Name (BGN) and RAP downlink backhaul mesh settings. In Cisco Catalyst 9800 Series Wireless Controller, you can also configure the maximum range of the MAPs, backhaul client access, and backhaul data rates.

These settings are configured for the global site in the **Create AP Profile** window. For more information, see Configure mesh settings for an AP profile for Cisco IOS XE devices, on page 429 and Configure mesh settings for an AP profile for Cisco AireOS devices, on page 434.

AP configuration

If you have existing APs that you want to use in the mesh network mode, you must first change the AP Mode to Bridge or Flex+Bridge using the **Configure Access Point** workflow. For information, see Configure APs, on page 1382.

After an AP is configured for Bridge or Flex+Bridge mode, the **AP 360** window shows the mesh configuration. At this point, you must provision the APs with the new configuration. For more information, see Provision Cisco APs on day 1, on page 627.

Note For Cisco Catalyst 9800 Series Wireless Controllers, during bulk mesh AP provisioning across floors, we recommend that you don't update these configurations simultaneously on already provisioned APs:

- Mesh role on the AP and mesh configuration (**Bridge Group Name**, **Range - Root AP to Mesh AP (in feet)**, **Backhaul Client Access**) on the AP profile
- Mesh role on the AP and AP profile or flex profile mapping with the site tag

If you simultaneously update these configurations during bulk mesh AP provisioning, you must do one of these tasks:

- Reprovision the Cisco Catalyst 9800 Series Wireless Controller. APs reboot after reprovisioning the wireless controller. After the reboot is complete, you can reprovision the APs with the required mesh role change.
- Reprovision one of the APs that has the updated mesh configuration. The other APs with the updated mesh configuration also reboot. After the reboot is complete, you can reprovision the APs with the required mesh role change.

Configure a certificate revocation check

Use this procedure to configure a certificate revocation check for the controller certificate.

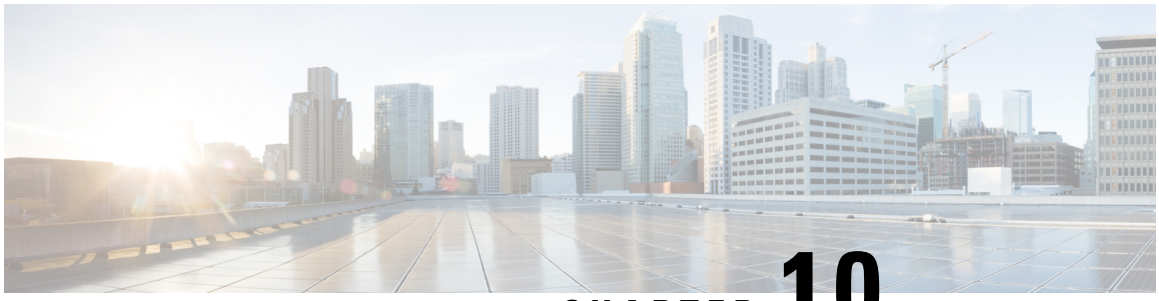
Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Security and Trust**.

Step 2 From the left hierarchy tree, select a site, building, or floor.

Step 3 In the **Revocation Check** drop-down list, **Revocation - Check: CRL None** is selected by default.

Step 4 To skip the revocation check, choose **Revocation - Check: None** and click **Save**.



CHAPTER 10

Configure Network Profiles

- Network profiles overview, on page 453
- Create network profiles for assurance, on page 453
- Create network profiles for firewall, on page 455
- Create network profiles for routing, on page 456
- Create network profiles for switching, on page 459
- Create network profiles for wireless, on page 460

Network profiles overview

Network profiles allow you to configure settings and apply them to a specific site or group of sites. You can create network profiles for various elements in Catalyst Center:

- Create network profiles for assurance, on page 453
- Create network profiles for firewall, on page 455
- Create network profiles for routing, on page 456
- Create network profiles for switching, on page 459
- Create network profiles for wireless, on page 460

Create network profiles for assurance

Creating a network profile for Assurance allows you to configure issue settings and apply them to a site or group of sites independently from the global issues settings. You can enable or disable an issue, and you can change its priority.

Note

- In Assurance, synchronization to the network device health score is available only for global issue settings, not custom issue settings. For information, see the *Cisco Catalyst Assurance User Guide*.
- Some global issues are not customizable. These issues are not displayed in the list of custom issues for you to modify.
- To display modified issues at the top of the list, sort by **Last Modified**.
- To delete custom settings, you must first unassign all the sites.

Procedure

Step 1 From the main menu, choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Assurance**.

Step 3 In the **Profile Name** field, enter a valid profile name and click **Next**.

Catalyst Center adds the profile and the **Edit Profile** window appears.

Step 4 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

Step 5 Click an issue in the **Issue Name** column to open a slide-in pane with the settings.

Note For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, Catalyst Center displays a caution that indicates the affected device types.

Step 6 To enable or disable whether Catalyst Center monitors the issue, click the **Enabled** toggle button.

Step 7 To set the issue priority, click the **Priority** drop-down list and choose the priority:

- **P1**: A critical issue that needs immediate attention and can have a wide impact on network operations.
- **P2**: A major issue that can potentially impact multiple devices or clients.
- **P3**: A minor issue that has a localized or minimal impact.
- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Step 8 (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
Memory Utilization of Access Points greater than 90%.
```

Step 9 (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default settings. Click **Use Default** to restore all the issue settings to the default values.

Step 10 Click **Apply**.

Step 11 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered.

Step 12 To assign the profile to sites, click **Assign Sites**. Check the check box next to the sites that you want to associate with this profile and click **Save**.

The **Edit Profile** window appears.



Note You can select a parent node or the individual sites. If you select a parent node, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

Step 13 Click **Done**.

The newly added profile appears on the **Network Profiles** window.

Create network profiles for firewall

This workflow shows how to:

1. Create profiles for Adaptive Security Appliance (ASA) devices and view the profile summary.
2. Create profiles for Firepower Threat Defense (FTD) devices and view the profile summary.

Procedure

Step 1 From the main menu, choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Firewall**.

The **Add Firewall Profile** page appears.

Step 3 To create ASA profiles, complete these steps:

a) In the **Name** field, enter the profile name.

b) Choose the number of devices from the **Devices** drop-down list.



Note You can choose up to 10 devices per profile.

c) Choose the type of device from the **Device Type** drop-down list.

d) (Optional) From the **Device Tag** drop-down list, choose the device tags.

e) Click **Next**.

The **Custom Configuration** page appears.

f) From the **Day-N Templates** drop-down list, choose a ASA template.

Note If there are no templates, you must create at least one template in **Design** > **CLI Templates**. For information, refer to Create templates, on page 486.

g) Click **Next**.

The **Summary** page appears. This page summarizes the custom configurations. Based on the selected device type, the page provides a hardware recommendation.

h) Click **Save**.

The **Network Profiles** page appears.

i) To assign a site to the network profile, click **Assign Sites**. For more information, refer to Create, edit, and delete a site, on page 240.

Step 4 To create FTD profile, complete these steps:

a) In the **Name** field, enter the profile name.

b) From the **Devices** drop-down list, choose the number of devices.

Note You can choose up to 10 devices per profile.

c) To provision an FTD firewall, check the **FTD** check box.

d) From the **Device Type** drop-down list, choose the type of device.

e) (Optional) Choose the device tags from the **Device Tag** drop-down list.

f) Click **Next**.

The **FTD Configuration** page appears.

g) Click the **Routed Mode** or **Transparent Mode** radio button.

h) Click **Next**.

The **Summary** page appears. This page summarizes the FTD configurations. Based on the selected device type, the page provides hardware recommendations.

i) Click **Save**.

The **Network Profiles** page appears.

j) To assign a site to the network profile, click **Assign Sites**. For information, refer to Create, edit, and delete a site, on page 240.

Create network profiles for routing

This workflow shows how to:

1. Add details for a router WAN configuration.
2. Add details for a router LAN configuration.

3. Add details for an integrated switch configuration.
4. Add a custom configuration.
5. View the profile summary.

Procedure

Step 1 From the main menu, choose **Design** > **Network Profiles**.

Step 2 Hover your cursor over **+ Add Profile** and choose **Routing**.

Step 3 The **Router WAN Configuration** page displays.

- Enter the profile name in the **Name** text box.
- Choose the number of **Service Providers** and **Devices** from the respective drop-down lists. Supports up to three service providers and ten devices per profile.
- Choose the **Service Provider Profile** from the drop-down list. For more information, refer to Configure service provider profiles, on page 350.
- Choose the **Device Type** from the drop-down list.
- Enter a unique string for the **Device Tag** to identify the different devices or choose an existing tag from the drop-down list. Use the device tag if two or more devices are of the same type. If all the devices are of a different type, the device tag is optional. Make sure to choose the appropriate tag. Part of the matching criteria for day-zero and day-*n* templates that apply to the network profile uses your selection.
- To enable at least one line link for each device to proceed, click the connection icon and check the check box next to **Connect**. Choose the **Line Type** from the drop-down list. Click **OK**.

  If you choose multiple service providers, you can choose:

  - **GigabitEthernet** for the primary interface and **Cellular** for the secondary interface,
  - **GigabitEthernet** for both interfaces, or
  - **Cellular** for the primary interface and **GigabitEthernet** for the secondary interface.

  Note The cellular interface only supports these integrated services routers:

  - Cisco 1100 Series
  - Cisco 4200 Series
  - Cisco 4300 Series
  - Cisco 4400 Series

- Click **Next**.

Step 4 The **Router LAN Configuration** page displays.

To skip the router LAN configuration, click the **Skip** radio button and continue to Step 5. To configure the router LAN:

- Click the **Configure Connection** radio button and choose **L2**, **L3**, or both.
- If you choose **L2**, click **+ Add Row**. Choose the **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**. You can add multiple rows by clicking **+ Add Row**, and you can delete rows by clicking **Delete**.
- If you choose **L3**, choose the **Protocol Routing** from the drop-down list and enter the **Protocol Qualifier**.
- Click **Next**.

Step 5 Based on your router configuration, the **Integrated Switch Configuration** page displays.

If the **Integrated Switch Configuration** page does not display, continue to Step 6.

The integrated switch configuration allows you to add new VLANs or retain the previously chosen configuration in the router LAN configuration.

- To add one or more new VLANs, click **+ Add Row**.
- Choose the **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- To delete a VLAN, click **Delete**.
- Click **Next**.



Note Switchport Interface support is available only for Cisco 1100 Series and Cisco 4000 Series integrated services routers.

Step 6 The **Custom Configuration** page displays.

Custom configurations are optional. You can skip this step and apply the configurations at any time in the **Network Profiles** window.

If you choose to add custom configurations:

a. Click the **Onboarding Template(s)** or **Day-N Template(s)** tab, as required.

b. Choose a template from the drop-down list. The templates filter by **Device Type** and **Tag Name**.

c. Click **Next**.

Step 7 On the **Summary** page, click **Save**.

This page summarizes the router configurations. If you have multiple devices, you can click on each device to view its configuration data. The page provides hardware recommendations based on the devices and chosen services.

Step 8 The **Network Profiles** window displays. In this window, you can edit and delete the network profiles.

Click **Assign Site** to assign a site to the network profile. For more information, refer to Create, edit, and delete a site, on page 240.

Create network profiles for switching

You can apply two types of configuration templates to a switching profile:

- Onboarding template
- Day-*n* template

Before you begin

Define the **Onboarding Configuration** template that you want to apply to the devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See Create Templates to Automate Device Configuration Changes, on page 483.

Procedure

Step 1 From the main menu, choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Switching**.

Step 3 In the **Add a Network Profile** page, enter the profile name in the **Profile Name** field.

Step 4 Click the tab for the template type that you want to associate with this profile.

If you want to associate ...	Then ...
an onboarding template,	click the **OnBoarding Template(s)** tab.
a day-*n* template,	click the **Day-N Template(s)** tab.

Step 5 Click **Attach Templates**.

Step 6 In the **Add Template** slide-in pane, complete these steps:

a) Under **Templates**, click a template name.

You can either search for a template by entering its name in the **Search** field, or expand a project and choose a template.

Note In previous Catalyst Center releases, you were able to associate a tag with a template. This functionality has been removed.

b) Click **Add**.

Step 7 Click **Save**.

The profile that is configured on the switch is applied when the switch is provisioned. You must add the network profile to a site for it to be effective.

Create network profiles for wireless

Before you begin

- Ensure that you have created wireless SSIDs, RF profiles, and AP profiles under the **Design** > **Network Settings** > **Wireless** tab.
- If necessary, ensure that you have created templates in the **Design** > **CLI Templates** window.
- If necessary, ensure that you have created feature templates in the **Design** > **Feature Templates** window.

Procedure

Step 1 From the main menu, choose **Design** > **Network Profiles**.

Step 2 Click **Add Profile** and choose **Wireless**.

Step 3 Enter a valid profile name in the **Profile Name** field.

Step 4 To add sites to the profile, click **Assign** and do these steps:

a) In the **Add Sites to Profile** slide-in pane, check the check box next to the sites that you want to associate with this profile.

You can select a parent node or the individual site. If you select a parent site, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

b) Click **Save**.

Step 5 Configure the required settings in these tabs:

- **SSIDs**: For more information, see Add SSIDs to a network profile, on page 460.
- (Optional) **AP Zones**: For more information, see Add AP zones to a network profile, on page 463.
- **Feature Templates**: For more information, see Add feature templates to a network profile, on page 464.
- **Templates**: For more information, see Add templates to a network profile, on page 465.
- (Optional) **Advanced Settings**: For more information, see Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475 and Configure additional interfaces for a network profile, on page 478.

Step 6 Click **Save** to add the network profile.

Catalyst Center displays the new network profile on the **Design** > **Network Profiles** window.

Add SSIDs to a network profile

You can add SSIDs to a network profile.

Before you begin

Ensure that you have created wireless SSIDs under the **Design** > **Network Settings** > **Wireless** > **SSIDs** window.

Procedure

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **SSID** tab.

Step 2 Click **Add SSID**.

Step 3 From the **SSID** drop-down list, choose the SSID that you have already created.

Step 4 (Optional) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Note

- If an SSID associated with a network profile doesn't have site-level overrides on the **Design** > **Network Settings** > **Wireless** window, Catalyst Center uses the WLAN profile name available in the network profile during provisioning.
- If you must associate an SSID that has site-level overrides on the **Design** > **Network Settings** > **Wireless** window (for configurations such as fabric, FlexConnect, guest anchor, user interfaces, scheduler, and so on) with multiple network profiles, ensure that the WLAN profile name is unique for the SSID across all network profiles to prevent provisioning failure.
- If an SSID associated with a network profile has site-level overrides, Catalyst Center uses the WLAN profile name or policy profile name from the overridden SSID during wireless controller provisioning for the corresponding sites. This rule applies when the overridden site is associated with the wireless controller's network profiles and is managed by the same wireless controller.
- If you modify the WLAN profile name for an existing SSID that is provisioned on a wireless controller, during the wireless controller reprovisioning, this SSID is deleted and recreated with the new WLAN profile name.
- When you upgrade to this release from a release earlier than Release 2.3.5, Catalyst Center populates the provisioned WLAN profile name and policy profile name to the corresponding existing SSIDs.

Step 5 (Optional) In the **Policy Profile Name** field, change the policy profile name.

By default, Catalyst Center automatically copies the WLAN profile name as the policy profile name.

Step 6 (Optional) Use the **Copy to Policy Profile Name** check box for one of these options:

- Automatically copy the WLAN profile name as the policy profile name.
- Enter a different name for the policy profile.

Step 7 (Optional) From the **802.11be Profile Name** drop-down list, choose an 802.11be profile.

By default, the default-dot11be-profile 802.11be profile is used. This profile is applicable for wireless controllers running Cisco IOS XE Release 17.15.2 or later.

The wireless controllers that run a version earlier than Cisco IOS XE Release 17.18.1 use only one dot11be-profile, which is the default-dot11be-profile. When you choose a 802.11be profile, the corresponding attributes map to the default-dot11be-profile on the wireless controller.

The wireless controllers that run Cisco IOS XE Release 17.18.1 or later support custom 802.11be profiles. You can use multiple 802.11be profiles across SSIDs in a network profile for a wireless controller.

For more information about 802.11be profiles, see Create an 802.11be profile, on page 446.

Step 8 Specify whether the SSID is fabric or nonfabric using the **Yes** or **No** radio buttons.

To create a nonfabric SSID, click **No**, and configure these parameters:

- Click the **Enable SSID Scheduler** toggle button and choose the scheduler from the drop-down list.
- To use an interface for traffic switching, click the **Interface** radio button. From the **Interface Name** drop-down list, choose an interface name for the SSID, or click the plus icon to create a wireless interface.
- To use a VLAN group for traffic switching, click the **VLAN Group** radio button. From the **VLAN Group Name** drop-down list, choose a VLAN group name for the SSID, or click the plus icon to create a VLAN group.
- In the **Do you need Anchor for this SSID?** area, click **Yes** to add an anchor to the SSID. By default, **No** is the selection.
- If you choose **Yes**, from the **Select Anchor Group** drop-down list, choose an anchor group for the SSID. For more information about anchor groups, see Create an anchor group, on page 422.
- If you choose **No**, check the **Flex Connect Local Switching** to enable local switching for WLAN.

  If you add an anchor to the SSID, you can't enable **Flex Connect Local Switching**.

  Note If you change any nonflex SSID that is already provisioned on the wireless controller to flex SSID (or the reverse), you must reprovision the wireless controller. Otherwise, the expected intent isn't configured on the wireless controller. For example, if you don't reprovision the wireless controller after changing a nonflex SSID to a flex SSID, the SSID remains nonflex on the wireless controller and flex site tags aren't created.

  If you enable **Flex Connect Local Switching** for an SSID, all the APs on the floor where the network profile is mapped, switch to FlexConnect mode.

  The **Flex Group** option is enabled in the **Advanced Settings** tab. For more information, see Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475.

  When you enable local switching, any FlexConnect AP that advertises this WLAN can locally switch data packets.

- If you have enabled the **Flex Connect Local Switching** check box, enter a value for the VLAN ID in the **Local to VLAN** field.

  Note When you modify the local VLAN ID of an existing SSID and reprovision the AP without reprovisioning the wireless controller, the latest value of the local VLAN ID updates in the flex profile that is used by the AP. If other APs use the same flex profile, they also have the local VLAN ID update.

Step 9 (Optional) To add another SSID, click the plus icon and configure its parameters.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create network profiles for wireless, on page 460.

Add AP zones to a network profile

An AP zone allows you to associate different SSIDs and RF profiles for a set of APs on the same site. You can use device tags to identify the APs for which you want to apply AP zone. From the **AP Zones** tab, you can create separate AP zones with a subset of SSIDs configured in the network profile for a device tag.

Catalyst Center applies the AP zone configurations to APs during AP provisioning.

Note

- If an AP zone is already provisioned on an AP and you update the AP zone configuration, you must reprovision the wireless controller. Reprovisioning the AP is not necessary.
- Catalyst Center supports AP zone optimization. When you upgrade to Release 3.2.2 from an earlier release, reprovision Cisco Catalyst 9800 Series Wireless Controllers to enable this optimization. If there are no other intent changes, reprovisioning the wireless controllers does not push new configurations to devices.

  For more information about reprovisioning the wireless controller, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

During AP provisioning:

- Based on the device tag and site of the AP, Catalyst Center selects the corresponding AP zone and automatically assigns the RF profile.
- If two AP zones are configured for an AP, you can choose the required AP zone.
- If there are no AP zones for an AP, you can choose the required RF profile.

Before you begin

Ensure that you have created wireless SSIDs under the **Design** > **Network Settings** > **Wireless** > **SSIDs** window.

Procedure

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **AP Zones** tab.

Step 2 Click **Add AP Zone**.

Step 3 In the **AP Zone Name** field, enter a name for the AP zone.

Step 4 From the **Device Tags** drop-down list, check the check box next to the device tags that you want to choose.

Step 5 From the **RF Profile** drop-down list, choose an RF profile.

Step 6 From the **SSID** drop-down list, choose the SSIDs.

Step 7 (Optional) To add another AP zone, click the plus icon and configure its parameters.

What to do next

Configure the other necessary settings for the network profile. For more information, refer to Create network profiles for wireless, on page 460.

To apply the AP zone configuration to an AP:

1. Reprovision the wireless controller. For more information, refer to Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.
2. Provision the AP. For more information, refer to Provision Cisco APs on day 1, on page 627.

Add feature templates to a network profile

You can attach feature templates to a network profile.

Procedure

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **Feature Templates** tab.

Step 2 Click **Add Feature Template**.

Step 3 In the **Add Feature Template** slide-in pane, do these steps:

a. Click **Filter by Device Type(s)** and choose a device type.

You can either search for a device name by entering its name in the **Search** field, or expand **Switches and Hubs** or **Wireless Controller** and choose a device type.

b. Expand **Wireless** and choose the feature templates that you want to attach to this network profile.

You can use the **Search Feature Template Designs** field to filter the feature templates.

c. From the **Tags** drop-down list under **APPLICABILITY**, choose the applicable tags.

d. Click **Add**.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create network profiles for wireless, on page 460.

Add templates to a network profile

You can associate a template with a network profile.

Before you begin

You must create the necessary templates in the **Design** > **CLI Templates** window. For more information, see Create templates, on page 486.

Procedure

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), click the **Templates** tab.

Step 2 Do this task:

- To associate an onboarding template, click the **OnBoarding Template(s)** tab.
- To associate a day-*n* template, click the **Day-N Template(s)** tab.

Step 3 Click **Attach Templates**.

Step 4 In the **Add Template** slide-in pane, do these steps:

a) Under **Templates**, click a template name.

You can either search for a template by entering its name in the **Search** field, or expand a project and choose a template.

b) Click **Add**.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create network profiles for wireless, on page 460.

Overview of AP groups, flex groups, site tags, and policy tags

You can define custom names for AP groups, flex groups, site tags, and policy tags in the **Advanced Settings** tab of the **Design** > **Network Profiles** > **Wireless** window. For more information, see Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475.

Catalyst Center configures and applies the newly added custom names specified in the **Provision Group** settings of the **Advanced Settings** tab to the APs during AP provisioning.

Note

- AP group and flex group configurations are applicable to Cisco AireOS Wireless Controllers.
- Site tag and policy tag configurations are applicable to Cisco Catalyst 9800 Series Wireless Controllers.

  Newly added site tag and policy tag configurations are applied when you provision the APs. Provisioning the wireless controller alone doesn't configure the new custom tags on the APs. You must reprovision the wireless controller or the APs if there are any modifications to the tags after provisioning.

  Consider these scenarios while provisioning or reprovisioning the wireless controller and APs:

  - If there are no custom site or policy tags configured on the network profile, Catalyst Center uses the autogenerated tags and configures it on the wireless controller and applies the changes to the APs only during AP provisioning.
  - If there are custom site or policy tags configured on the network profile, Catalyst Center configures the custom tags on the wireless controller and applies the changes to the APs only during AP provisioning.
  - If the wireless controller and AP are already provisioned with autogenerated tags and if you create new custom tags in the network profile, you must reprovision the wireless controller or the AP to apply the changes.
  - If the wireless controller and AP are already provisioned with custom tags and if you delete the custom tags from the network profile, you must reprovision the wireless controller or the APs.
    - Reprovisioning the wireless controller deletes the custom tag configurations and configures the autogenerated tags on the wireless controller and the associated APs.
    - Reprovisioning the APs directly, without reprovisioning the wireless controller, configures the autogenerated tags on the APs but doesn't delete the custom tag configurations from the wireless controller. The tags are deleted during the next wireless controller reprovisioning.
  - If you've upgraded to Catalyst Center with FlexConnect Native VLAN override configured and site tags that are mapped to the same custom Flex profile for all the floors in a site, you must reconfigure the network profile with different site tags for each floor or else provisioning may fail.

You can use the same AP groups and flex groups across sites (buildings or floors) across multiple areas. Child sites inherit the AP groups and flex groups from their parent sites. However, if you create AP groups or flex groups for a child site, it overrides the settings inherited from its parent site. If an SSID is overridden for different floors in a building, you can't reuse the AP groups or flex groups for such floors. For AP group and flex group reuse examples, see Custom AP group and flex group reuse examples, on page 469.

Consider these scenarios while using the same AP groups and flex groups across multiple sites:

- You must configure the same RF profile for the shared AP groups.

  For example, the custom AP group *AP-Group-1* is shared across *Network-Profile-1* and *Network-Profile-2*. It's managed by the same wireless controller with the same AP zone name (default or custom AP zone). If *Network-Profile-1* uses *RF-Profile-1* and *Network-Profile-2* uses *RF-Profile-2*, a validation error occurs during provisioning. You must configure the same RF profile for *AP-Group-1*.

- You must configure the same AP zone name for the shared custom AP groups.

For example, the custom AP group *AP-Group-1* is shared across *Network-Profile-1* and *Network-Profile-2*. Both network profiles use the same RF profile *RF-Profile-1*. If *Network-Profile-1* uses the AP zone *default-zone* and *Network-Profile-1* uses *AP-Zone-1*, a validation error occurs during provisioning. You must configure the same AP zone name for *AP-Group-1*.

- For shared custom AP groups, if any site with active APs is removed and the RF profile is also modified simultaneously, do one of these tasks before reprovisioning the APs:
  - Create another custom AP group and reprovision the APs in the sites that are removed from the custom AP group.
  - Reprovision the APs without creating a custom AP group so that the AP uses the Catalyst Center-generated AP group. Later, reprovision the APs with the updated RF profile and the shared custom AP group.

  For example, the custom AP group *AP-Group-1* that uses *RF-Profile-1* is shared across *Building-1*/*Floor-1* and *Building-2*/*Floor-2*. When you provision APs on *Building-1*/*Floor-1* and *Building-2*/*Floor-2*, the APs join *AP-Group-1* on both the floors. If you change the RF profile to *RF-Profile-2* and simultaneously remove *Building-2*/*Floor-2* from *AP-Group-1*, a validation error occurs during provisioning. You must reprovision the APs on *Building-2*/*Floor-2* to move them to the required AP group. Later, reprovision APs on *Building-1*/*Floor-1*.

- For shared custom AP groups, if the AP zone name is changed, you must reprovision the existing APs in the old AP zone. Later, reprovision the APs with the new AP zone and the custom AP group.

  For example, *Network-Profile-1* is assigned to *Building-1*/*Floor-1* with *AP-Group-1*, *RF-Profile-1*, and *AP-Zone-1*. *Network-Profile-2* is assigned to *Building-2*/*Floor-2* with *AP-Group-1*, *RF-Profile-1*, and *AP-Zone-1*. The managed AP location for the *Wireless-Controller-1* is configured as *Building-1* and *Building-2*. *AP1* is provisioned on *Building-1*/*Floor-1* and *AP2* is provisioned on *Building-2*/*Floor-2*. If you change the AP group to *New-AP-Group* and AP zone to *AP-Zone-3* on both *Network-Profile-1* and *Network-Profile-2*, and reprovision *AP1* or *AP2* with *AP-Zone-3* on the corresponding floors, a validation error occurs. You must reprovision *AP1* and *AP2* with *AP-Zone-1*. Later, reprovision *AP1* and *AP2* with *AP-Zone-3* and *New-AP-Group*.

- For shared custom AP groups, if you modify the AP zone on a parent site, these modifications are also inherited by the child sites. You must create the required AP zone on the network profile assigned to the child site.



Note If the child site has overridden configurations, the configurations aren't overwritten.

For example, *Building-1* contains child sites *Floor-1* and *Floor-2*. *Network-Profile-1* is assigned to *Building-1* and *Floor-1*, and *AP-Group-1*, *AP-Zone-1*, and *RF-Profile-1* are configured for *Building-1*. *Network-Profile-2* is assigned to *Floor-2*, and *AP-Group-1*, *AP-Zone-1*, and *RF-Profile-1* are configured for *Floor-2*. *AP1* is provisioned on *Floor-1* and *AP2* is provisioned on *Floor-2* with *AP-Zone-1*. AP zone configuration for *AP-Group-1* on *Building-1* is updated to use *AP-Zone-2* and *RF-Profile-2*. Since *Floor-2* inherits values from *Building-1*, any updates to the AP group settings on *Building-1* are automatically reflected in *Floor-2*. So, even though *APZone-2* doesn't exist in *Network-Profile-2*, it's updated in the *Floor-2* AP group settings due to inheritance. If you reprovision *AP1* on *Floor-1* with *AP-Zone-2*, a validation error occurs. You must create *AP-Zone-1* in *Network-Profile-2*.

- If a shared custom AP group is used across multiple sites but the SSID differs between those sites, AP provisioning fails. Catalyst Center does not support AP group reuse when SSID mappings are not identical across sites. To resolve this issue, create a unique custom AP group for the site that requires a different SSID, and then reprovision the APs.

  For example, the custom AP group *APGroup1* is configured on *Building-1*/*Floor-1* with *AP-Zone-1*, SSID *WLAN-1*, and RF profile *Typical*. *APGroup1* is also configured on *Building-1*/*Floor-2* with *AP-Zone-1*, SSID *WLAN-2*, and RF profile *Typical*. *AP1* is provisioned on *Floor-1* and uses *AP-Group-1*. If you provision *AP2* on *Floor-2* using *APGroup1*, a validation error occurs as the SSID mappings are different in these two sites. You must create a unique custom AP group for *Floor-2* before reprovisioning *AP2*.

- For shared custom AP groups, if you change the RF profile and reprovision the corresponding APs, the custom AP group is updated with the new RF profile across sites for all the APs using the custom AP group.

  For example, the custom AP group *AP-Group-1* is shared across *Network-Profile-1* and *Network-Profile-2*. *Network-Profile-1* is assigned to *Building-1*/*Floor-1* and uses *AP-Group-1* with *RF-Profile-1*. *Network-Profile-2* is assigned to *Building-2*/*Floor-2* and uses *AP-Group-1* with *RF-Profile-1*. The wireless controller is provisioned, and *AP1* is provisioned on *Building-1*/*Floor-1* and *AP2* is provisioned on *Building-2*/*Floor-2*. If you update the RF profile of *AP-Group-1* to *RF-Profile-2* in both nework profiles and reprovision *AP1* and *AP2*, *AP-Group-1* is updated to use *RF-Profile-2* on both *Floor-1* and *Floor-2*.

- You can't use the same flex group on multiple sites with different native VLAN or AAA override VLAN.

Custom policy tags can be reused across sites (areas, buildings, and floors). When you assign a custom policy tag to a site—an area, a building, or multiple floors in a building—all APs provisioned to that site and AP zone can use the same custom policy tag. By default, the custom policy tags are applicable for APs in the default AP zone; for custom AP zones, edit the policy tag and assign the custom policy tag to the required zones.

Note While reusing the custom policy tags:

- Child sites inherit the custom policy tags from the parent sites. However, if you create another policy tag for the child site, it overrides the settings inherited from the parent site.
- A custom policy tag can be assigned to multiple sites and multiple AP zones. All AP zones associated with the policy tag must share the same set of SSIDs and the SSIDs must have the same configuration. If a policy tag is associated to multiple AP zones that have different SSID configurations, an error is shown while editing the policy tag or the network profile.
- A custom policy tag can't be shared when any of the sites that share the custom policy tag and are managed by the same wireless controller have different SSID configurations due to a site-level SSID override. In such cases, a validation error occurs during provisioning—either AP provisioning or wireless controller provisioning (if the **Skip AP Provision** check box is unchecked) due to different WLAN profile and policy profile mappings for the same custom policy tag. An error message with the reason for failure is displayed in the configuration preview. The error message provides details for up to five sites that have a mismatch for the custom policy tag. For more information on the custom policy tag usage, see Custom policy tag reuse use case examples, on page 472.
- Policy tags are mapped to WLAN and RLAN profiles. Any changes in the policy tag may impact the RLAN configurations.
- Policy tag reuse isn't supported for Catalyst Center autogenerated tags.

Custom flex profiles are configured either during wireless controller provisioning or during AP provisioning accordingly:

- During wireless controller provisioning: If there's a flex feature template attached to the network profile, a custom flex profile or a Catalyst Center autogenerated flex profile (based on the option selected while configuring a custom site tag) is created during wireless controller provisioning. The custom flex profile is configured with the same settings as that of the default flex profile except for the Catalyst Center intent configurations as defined in the feature template with **IP Overlap** enabled. When you provision the AP after provisioning the wireless controller, the custom flex profile isn't overwritten except for the FlexConnect VLAN settings (Native VLAN and AAA Override VLAN), if configured.
- During AP provisioning: If there's no feature template attached to the network profile, a custom flex profile is created during AP provisioning. The custom flex profile is configured with the same settings as that of the default flex profile except for the FlexConnect VLAN settings (Native VLAN and AAA Override VLAN), if configured. Catalyst Center enables the pairwise master key (PMK) propagation in the custom flex profile during AP provisioning.

Custom AP group and flex group reuse examples

Scenario 1

A custom AP group and flex group are shared between multiple sites with no site overrides and all sites are managed by the same wireless controller.

Site	Site override	AP group, AP zone, and RF profile	Native VLAN ID override	Primary wireless controller
Area-1/Building-1/Floor-1	None	*Custom-AP-Group-1*, *default-zone*, *Typical*	None	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	None	*Custom-AP-Group-1*, *default-zone*, *Typical*	None	*Wireless-Controller-1*

In this scenario, the custom AP group and flex group can be shared between the sites and the APs can be successfully provisioned to these sites using the same custom AP group.

Scenario 2

A custom AP group is shared between multiple sites where some sites have site overrides for SSID and all the sites are managed by the same wireless controller.

Site	Site override	AP group, AP zone, and RF profile	Primary wireless controller
Area-1/Building-1/Floor-1	Site override - PSK changes	*Custom-AP-Group-1*, *AP-Zone-1*, *HIGH*	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	None	*Custom-AP-Group-1*, *AP-Zone-1*, *HIGH*	*Wireless-Controller-1*

In this scenario, the custom AP group can't be reused as it has different WLAN profile mapping for the same SSID. If you provision APs to these sites using the same custom AP group, a validation error occurs during provisioning.

Note The AP provisioning for the first site in this site hierarchy (*Area-1/Building-1/Floor-1*) is successful but a validation error is displayed during the second AP provisioning at *Area-2/Building-1/Floor-1*, which is attempting to reuse the custom AP group.

Scenario 3

A custom AP group is shared between multiple sites with different RF profiles and all the sites are managed by the same wireless controller.

Site	Site override	AP group, AP zone, and RF profile	Primary wireless controller
Area-1/Building-1/Floor-1	None	*Custom-AP-Group-1*, *AP-Zone-1*, *HIGH*	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	None	*Custom-AP-Group-1*, *AP-Zone-1*, *LOW*	*Wireless-Controller-1*

In this scenario, the custom AP group can't be reused as it has different RF profiles. If you provision APs to these sites using the same custom AP group, a validation error occurs during provisioning.

Note The AP provisioning for the first site in this site hierarchy (*Area-1/Building-1/Floor-1*) is successful but a validation error is displayed during the second AP provisioning at *Area-2/Building-1/Floor-1*, which is attempting to reuse the custom AP group.

Scenario 4

A custom AP group is shared between multiple sites where some sites have no site overrides for SSID for the primary controller, but has an override for the secondary controller.

Site	Site override	AP group, AP zone, and RF profile	Primary wireless controller	Secondary wireless controller
Building-1	None	*Custom-AP-Group-1*, *AP-Zone-1*, *HIGH*	*Wireless-Controller-1*	*Wireless-Controller-2*
Building-1/*Floor-1*	None	*Custom-AP-Group-1*, *AP-Zone-1*, *HIGH*	*Wireless-Controller-1*	*Wireless-Controller-2*
Building-1/*Floor-2*	None	*Custom-AP-Group-1*, *AP-Zone-1*, *HIGH*	*Wireless-Controller-1*	*Wireless-Controller-2*
Building-2/*Floor-1*	SSID override	*Custom-AP-Group-1*, *AP-Zone-1*, *LOW*	*Wireless-Controller-2*	None

In this scenario, the custom AP group can't be reused as it has different WLAN profile mapping for the same SSID for *Wireless-Controller-2*. If you provision APs to these sites using the same custom AP group, a validation error occurs during provisioning.

Note The AP provisioning for the first site in this site hierarchy (*Building-1/Floor-1*) is successful but a validation error is displayed during the second AP provisioning at *Building-2/Floor-1*, which is attempting to reuse the custom AP group.

Scenario 5

A custom AP group is shared between multiple sites with different sets of WLANs and all sites are managed by the same wireless controller.

Site	Site override	AP group, AP zone, and RF profile	Primary wireless controller
Area-1/Building-1/Floor-1	None	*Custom-AP-Group-1*, *AP-Zone-1* (*WLAN-1*, *WLAN-2*), *HIGH*	*Wireless-Controller-1*

Site	Site override	AP group, AP zone, and RF profile	Primary wireless controller
Area-2/Building-1/Floor-1	None	*Custom-AP-Group-1*, *AP-Zone-1* (*WLAN-3*, *WLAN-4*), *HIGH*	*Wireless-Controller-1*

In this scenario, the custom AP group can't be reused as it has different WLAN profile mapping for the same wireless controller. If you provision APs to these sites using the same custom AP group, a validation error occurs during provisioning.

Note The AP provisioning for the first site in this site hierarchy (*Area-1/Building-1/Floor-1*) is successful but a validation error is displayed during the second AP provisioning at *Area-2/Building-1/Floor-1*, which is attempting to reuse the custom AP group.

Custom policy tag reuse use case examples

Scenario 1

A custom policy tag is shared between multiple sites with no site overrides and all sites are managed by the same Cisco Wireless Controller.

Site	Site override	Policy tag and AP zone	Primary wireless controller
Building 1/Floor 1	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*
Building 1/Floor 2	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*

In this scenario, the custom policy tags can be shared between the sites and the APs can be successfully provisioned to these sites using the same custom policy tag.

Scenario 2

A custom policy tag is shared between multiple sites where some sites have site overrides for SSID and all the sites are managed by the same wireless controller.

Site	Site override	Policy tag and AP zone	Primary wireless controller
Building 1/Floor 1	Site Override	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*
Building 1/Floor 2	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*

In this scenario, the custom policy tag cannot be reused because the same tag has two different WLAN profile and policy profile mappings for the same SSID. If you provision APs to these sites using the same custom policy tag, a validation error occurs during provisioning.

Note The AP provisioning for the first site in this site hierarchy (*Building 1/Floor 1*) will be successful but a validation error is shown during the second AP provisioning at *Building 1/Floor 2*, which is attempting to reuse the custom policy tag.

Scenario 3

A custom policy tag is shared between multiple sites where some sites have site overrides for SSID and the sites are managed by different primary wireless controllers.

Site	Site override	Policy tag and AP zone	Primary wireless controller
Building 1/Floor 1	Site Override	*Custom Policy Tag 1*, *default-zone*	*wireless controller 2*
Building 1/Floor 2	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*

In this scenario, the custom policy tags can be reused and the APs can be successfully provisioned to these sites using the same custom policy tag.

Scenario 4

A custom policy tag is shared between multiple sites where some sites have no site overrides for the primary wireless controller and some sites have overrides for the secondary wireless controller. All the sites are managed by the same primary wireless controller and have N+1 HA configured.

Site	Site override	Policy tag and AP zone	Primary wireless controller	Secondary wireless controller
Building 1/Floor 1	No Override from Global level	*Custom Policy Tag 1*, *default -zone*	*wireless controller 2*	-
Building 2	Site Override	*Custom Policy Tag 1*, *default -zone*	*wireless controller 1*	*wireless controller 2*
Building 2/Floor 1	No Override from *Building 2*	*Custom Policy Tag 1*, *default -zone*	*wireless controller 1*	*wireless controller 2*
Building 2/Floor 2	No Override from *Building 2*	*Custom Policy Tag 1*, *default -zone*	*wireless controller 1*	*wireless controller 2*

In this scenario, since all the sites are managed by the same N+1 wireless controller, the custom policy tag cannot be reused for *wireless controller 2* because the same tag has two different WLAN profile and policy profile mappings for the same SSID on the same wireless controller (*wireless controller 2*). A validation error occurs when you provision *wireless controller 2*. However, there's no error expected while provisioning the *wireless controller 1*.

Note Validation is done independently for each of the wireless controllers.

Scenario 5

A custom policy tag is shared across areas with the same network profile.

Site	Site override	Policy tag and AP zone	Primary wireless controller
Area 1/Building 1/Floor 1	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*
Area 2/Building 2/Floor 1	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1 or 2*

In this scenario, custom policy tags can be shared across wireless controllers managing different areas under the same network profile.

Scenario 6

A custom policy tag is shared across areas with multiple network profiles.

Example 1

In this example, custom policy tag can be reused across areas with different network profiles.

Site	Network profile	Site override	Policy tag and AP zone	Primary wireless controller
Area 1/Building 1/Floor 1	*Profile 1*	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*
Area 2/Building 2/Floor 1	*Profile 2*	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1 or 2*

Example 2

In this example, the custom policy tag cannot be reused due to site override in *Area 2*.

Site	Network profile	Site override	Policy tag and AP zone	Primary wireless controller
Area 1/Building 1/Floor 1	*Profile 1*	None	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1*
Area 2/Building 2/Floor 1	*Profile 2*	Site Override in *Area 2*	*Custom Policy Tag 1*, *default-zone*	*wireless controller 1 or 2*

Scenario 7

A custom policy tag is shared across multiple AP zones.

Example 1

In this example, the same custom policy tag can be reused across two AP zones (*workarea*, *corridor*) when they have the same set of SSID (*SSID 1*).

Site	Site override	Policy tag and AP zone	Primary wireless controller
Area 1/Building 1/Floor 1	None	*Custom Policy Tag 1*, *workarea (SSID 1)*	*wireless controller 1*
Area 2/Building 2/Floor 1	None	*Custom Policy Tag 1*, *corridor (SSID 1)*	*wireless controller 1*

Example 2

In this example, the custom policy tag cannot be reused because the AP zones do not have the same set of SSIDs.

Site	Site Override	Policy Tag and AP Zone	Primary wireless controller
Area 1/Building 1/Floor 1	None	*Custom Policy Tag 1*, *workarea (SSID 1, SSID 2)*	*wireless controller 1*
Area 2/Building 2/Floor 1	None	*Custom Policy Tag 1*, *corridor (SSID 1)*	*wireless controller 1*

Note Reconfiguring a shared custom policy tag (for example, swapping the AP zone for a policy tag with another tag) results in conflicting configurations for existing APs on different floors that are yet to be reprovisioned. This prevents provisioning because the APs that are yet to be provisioned are still using the old configuration. However, reconfiguration of a shared custom policy tag is allowed in cases where all the APs that share the tag are on the same floor. The APs are updated with the latest configuration when you reprovision the APs of all the zones.

Add AP groups, flex groups, site tags, and policy tags to a network profile

Catalyst Center allows you to add AP groups, flex groups, site tags, and policy tags in a network profile. Adding AP groups and flex groups saves time during AP provisioning by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. If you don't configure the custom names, Catalyst Center uses the autogenerated AP group names and tags for the APs.

Note Flex group configuration is available only when the network profile has at least one associated flex-based SSID.

Before you begin

- Ensure that you have assigned a site to the network profile.

- To create flex group names, under the **SSIDs** tab, ensure that you have checked the **Flex Connect Local Switching** check box and defined the VLAN ID in the **Local to VLAN** field to mark the nonfabric SSID as a flex-based SSID. For more information, see Add SSIDs to a network profile, on page 460.

  If you have enabled **Flex Connect Local Switching** for an SSID, all the APs on the floor where the network profile is mapped, switch to FlexConnect mode.

- For information about reprovisioning the wireless devices, and using the groups and tags, see Overview of AP groups, flex groups, site tags, and policy tags, on page 465.

Procedure

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), hover your cursor over **Advanced Settings** and click **Provision Group**.

Step 2 (Optional) To create an AP group in the network profile, expand **AP Groups and AP Profiles** and click **Create Custom AP Group**.

In the **Add AP Group** slide-in pane, do these steps:

a) In the **AP Group Name** field, enter the AP group name.
b) From the **AP Zone** drop-down list, choose an AP zone.

To broadcast all the SSIDs associated with the network profile, choose **Not Applicable**.

Note This drop-down list is enabled if you have added AP zones to the network profile in the **AP Zones** tab. For more information, see Add AP zones to a network profile, on page 463.

If you choose an AP zone, the RF profile is inherited from the AP zone configuration.

c) From the **AP Profile** drop-down list, choose an AP profile.

To create an AP profile, click **Create New**. For more information, see AP profiles, on page 424.

d) From the **RF Profile** drop-down list, choose an RF profile.

Note This drop-down list is disabled if you choose an AP zone from the **AP Zone** drop-down list.

e) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.
f) Click **Save**.

Step 3 (Optional) To create a flex group in the network profile, expand **Flex Group** and click **Create Flex Group**.

In the **Create Flex Group** slide-in pane, do these steps:

a) In the **Flex Group Name** field, enter the flex group name.
b) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.
c) Click **Save**.

Step 4 (Optional) To create a site tag in the network profile, expand **Site Tags and AP Profiles** and click **Create Custom Site Tag**.

In the **Create Site Tag** slide-in pane, do these steps:

a) In the **Site Tag Name** field, enter the site tag name.

You can enter up to 32 alphanumeric characters, special characters, and spaces. Catalyst Center supports these characters in the site tag name:

- ASCII characters: from 32 to 126
- Special characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Catalyst Center does not support <, /, '.*', ? and leading or trailing spaces in the site tag name.

b) From the **AP Profile** drop-down list, choose an AP profile.

To create an AP profile, click **Create New**. For more information, see AP profiles, on page 424.

c) In the **Load** field, enter a load value for the site tag. Valid range is 0 to 1000.

You can set the load value based on the number of access points. When you set a value, the new load configurations are pushed to the wireless controller during reprovisioning. These configurations take effect only after the access points disconnect and reconnect, or after you reboot the wireless controller. If you do not configure a load value, the existing load configurations on the wireless controller remain unchanged.

d) In the **Flex Profile Name** field, enter the flex profile name.



Note To enable the **Flex Profile Name** field, in the **SSID** tab, check the **Flex Connect Local Switching** check box. For more information, see Add SSIDs to a network profile, on page 460.

To use a Catalyst Center autogenerated name, check the **Auto generate Flex Profile Name** check box.

e) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.

You can select multiple areas under an area.

f) Click **Save**.

Step 5 (Optional) To create a policy tag in the network profile, expand **Policy Tag** and click **Create Policy Tag**.

In the **Create Policy Tag** slide-in pane, do these steps:

a) In the **Policy Tag Name** field, enter the policy tag name.

You can enter up to 31 alphanumeric characters, special characters, and spaces. Catalyst Center supports these characters in the policy tag name:

- ASCII characters: from 32 to 126
- Special characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Catalyst Center does not support <, /, '.*', ? and leading or trailing spaces in the policy tag name.

b) From the **AP Zone** drop-down list, choose an AP zone.

Note This drop-down list is enabled if you have added AP zones to the network profile in the **AP Zones** tab. For more information, see Add AP zones to a network profile, on page 463.

c) In the **Select Sites** area, you can either search for a site by entering its name or expand **Global** to choose a site.
d) Click **Save**.

What to do next

Configure the other necessary settings for the network profile. For more information, see Create network profiles for wireless, on page 460.

Configure additional interfaces for a network profile

An additional interface on a Cisco Wireless Controller maps a WLAN to a VLAN or subnet. You can configure additional interfaces for a network profile for wireless.

Procedure

Step 1 In the **Add a Network Profile** window (**Design** > **Network Profiles** > **Add Profile** > **Wireless**), hover your cursor over **Advanced Settings** and click **Additional Interface**.

Step 2 To create an additional interface, click **Create New Interface** and do these steps:

a) In the **Interface Name** field of the **Add Interface** slide-in pane, enter a name for the interface.
b) In the **VLAN ID** field, enter a VLAN ID.

For Cisco AireOS Wireless Controllers, the valid range is from 1 through 4094. For Cisco Catalyst 9800 Series Wireless Controllers, the valid range is from 2 through 4094.

c) Click **Save**.

Alternatively, you can create an additional interface on the **Design** > **Network Settings** > **Wireless** > **Interfaces & VLAN Groups** > **Interfaces** window. For more information, see Create a wireless interface, on page 381.

Step 3 To add additional interfaces to a network profile, do one of these tasks

- Click the plus icon next to the required additional interface.
- Click the additional interface name, and then click **Add Selected**.

Note To choose multiple additional interfaces, press **Shift**, click the additional interface names, and then click **Add Selected**.

- To add all the additional interfaces, click **Add All**. You can use the **Search** field to filter the additional interfaces.

What to do next

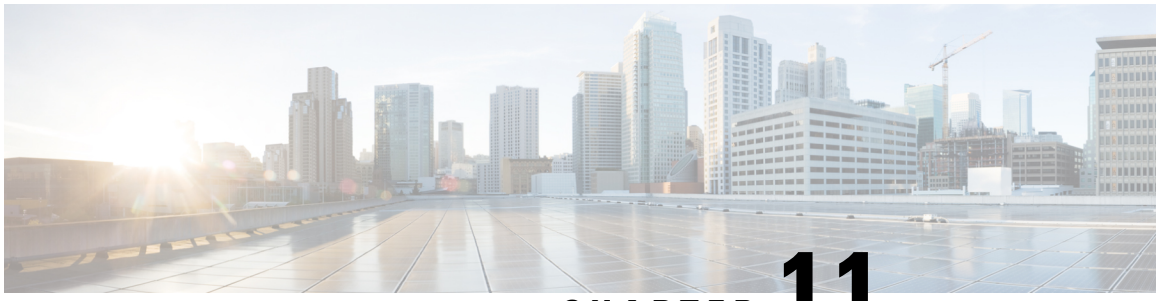
After configuring the necessary settings for the network profile, click **Save**. For more information, refer to Create network profiles for wireless, on page 460.



PART IV

Configure and Maintain Network Devices

- Create Templates to Automate Device Configuration Changes, on page 483
- Design Feature Templates, on page 509
- Manage Software Images, on page 533
- Compliance Audit for Network Devices, on page 561
- Run Diagnostic Commands on Devices, on page 581



CHAPTER 11

Create Templates to Automate Device Configuration Changes

- About CLI Templates, on page 483
- Onboarding templates or day-zero templates, on page 485
- Deploy configurations on the network devices with day-*n* templates, on page 485
- Create projects, on page 486
- Create templates, on page 486
- Export templates, on page 493
- Import templates, on page 493
- Clone a template, on page 494
- Attach a CLI template to the network profiles, on page 495
- Provision CLI templates, on page 495
- Export projects, on page 496
- Import projects, on page 497
- Template variables, on page 497
- Associate templates to network profiles, on page 504
- Detect conflicts in a CLI template, on page 506

About CLI Templates

Catalyst Center provides an interactive **CLI Templates** window to author your CLI templates. You can design templates easily with a predefined configuration by using parameterized elements or variables. After creating a template, you can use the template to deploy your devices in one or more sites that are configured anywhere in your network.

With CLI Templates, you can:

- View the list of available templates.
- Create, edit, clone, import, export, and delete a template.
- Filter the template based on the **Project Name**, template **Type**, **Template Language**, **Category**, **Device Family**, **Device Series**, **Commit State** and **Provision Status**.
- View these template attributes in **Design** > **CLI Templates** window in the **Templates** table:
  - **Name**: Name of the CLI template.

- **Project**: Project under which the CLI template is created.
- **Type**: Type of CLI template (regular or composite).
- **Version**: Number of versions of the CLI template.
- **Commit State**: The latest version of the template committed. You can view this information under the **Commit State** column:
  - The timestamp of the last committed date.
  - A warning icon means the template is modified but not committed.
  - A check icon means the latest version of the template is committed.



Note The last template version must be committed to provision the template on the devices.

- **Provision Status**: Viewable information under the **Provision Status** column:
  - The number of devices on which the template is provisioned.
  - A check icon displays the number of devices for which the CLI template was provisioned without any failures.
  - A warning icon displays the number of devices for which the latest version of the CLI template is not yet provisioned.
  - A cross icon displays the number of devices for which the CLI template deployment failed.
- **Potential Design Conflicts**: Potential conflicts in the CLI template.
- **Network Profiles**: The number of network profiles attached to a CLI template. In the **Network Profiles** column, click **Attach** to attach a CLI template to network profiles.
- **Actions**: In the **Actions** column, hover your cursor over the ellipsis icon to clone, commit, delete, or edit a template; edit a project; or attach a template to a network profile.

- Add interactive commands.
- Autosave the CLI commands.
- Version control the templates for tracking purposes.

  View the versions of a CLI template in **CLI Templates**, click the template name and click the **Template History** tab to view the template version.
- Detect errors in templates.
- Simulate templates.
- Define variables.
- Detect run-time conflict.

Note

- Make sure your template does not overwrite a network-intent configuration pushed by Catalyst Center.
- Use feature templates (intent-based) for configurations like IP MAC binding.

Onboarding templates or day-zero templates

Onboarding templates in Catalyst Center are used to automate the initial provisioning and onboarding process on the network devices. Onboarding templates define the configuration settings that should be applied to a device during the onboarding process.

Onboarding templates are primarily used with Plug and Play (PnP) to streamline the deployment of new network device in the network.

For example, you have a set of new switches that you want to deploy in your network. With an onboarding template, you can define the initial configuration settings, such as interface configurations, VLAN assignments, and basic security settings that should be applied to these switches during the onboarding process. When you connect the new switches to the network, Catalyst Center will automatically detect them using PnP and apply the defined configuration settings from the onboarding template, ensuring consistent and standardized configurations across your network.

Note

- Day-zero template is pushed as part of PnP.
- Day-zero templates are not allowed to bind to source or system variables, that is, the templates will not have the option to bind or use variables in the template with the source object values while editing or through the input form enhancements; for example, DHCP server, DNS server, and syslog server.
- Day-zero templates does not support the usage of special keywords that are described in the section Special keywords, on page 502.
- It is recommended to ensure that you are using the correct configuration in the day-zero template, as day-zero template pushes the entire configuration as it is, including the incorrect line.

Deploy configurations on the network devices with day-*n* templates

You can use day-*n* templates to apply configurations to the network devices, after devices have been added to the inventory. Day-*n* templates in Catalyst Center are used for configuration management and consistency across your network devices.

Day-*n* templates are designed for simplifying the process of making configuration changes, pushing firmware updates, or deploying network-wide policy changes to multiple devices at the same time. Day-*n* templates capture a specific configuration state or change that you want to apply to one or more devices. For configurations that can't be completed using the intent configurations in Catalyst Center, you can use the day-*n* templates.

Day-*n* templates are associated to a network profile as described in section Attach a CLI template to the network profiles, on page 495. The templates are applied to the devices during device provisioning. A device can be provisioned multiple times. By default, only new configuration is pushed during re-provisioning, but this setting can be overridden.

For example, you want to deploy a new Access Control List (ACL) on a group of switches in your network to enforce a security policy. With a day-*n* template, you can define the ACL configuration and apply it to the targeted switches. Catalyst Center will push the configuration to the devices, ensuring consistent application of the ACL across the network. If you need to update the ACL in the future, you can make changes to the day-*n* template, and Catalyst Center will push those changes to the devices accordingly.



Note

- The day-*n* templates are compiled and stored in Catalyst Center but their configurations are delivered to the devices in inventory through multiple concurrent SSH sessions. So the commands are sent to the devices line-by-line.
- If the day-*n* template contains an incorrect configuration, when such line is pushed to the device and fails, it stops Catalyst Center from applying the rest of the template.

Create projects

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 Click **Add** and then choose **New Project**.

The **Add New Project** slide-in pane displays.

Step 3 Enter a unique name in the **Project Name** field.

Step 4 (Optional) Enter a description for the project in the **Project Description** field.

Step 5 Click **Continue**.

The project is created and appears in the left pane.

What to do next

Add a new template to the project. For more information, see Create a regular template, on page 487 and Create a composite template, on page 489.

Create templates

Templates provide a method to easily predefine configurations using parameter elements and variables. Templates allow an administrator to define a configuration of CLI commands that can be used to consistently

configure multiple network devices, reducing deployment time. Variables in the template allow customization of specific settings per device.

Create a regular template

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Note By default, the **Onboarding Configuration** project is available for creating day-zero templates. You can create your own custom projects. Templates, created in custom projects, are categorized as day-*n* templates.

Step 2 In the left pane, click **Project Name** and choose the project under which you are creating templates.

Step 3 Click **Add** and then choose **New Template** from the drop-down list.

Note The template that you create for day zero can also be applied for day *n*.

Step 4 In **Add New Template** slide-in pane, configure the settings for the regular template.

In the **Template Details** area, do these steps:

a. Enter a unique name in the **Template Name** field.

b. Choose the **Project Name** from the drop-down list.

c. **Template Type**: Click **Regular Template**.

d. **Template Language**: Choose either the **Velocity** or **Jinja** language to use for the template content.

- **Velocity**: Use the Velocity Template Language (VTL). For information, see http://velocity.apache.org/engine/devel/vtl-reference.html.

  The Velocity template framework restricts the use of variables that start with a number. Make sure that the variable name starts with a letter and not with a number.

  Note Do not use the dollar ($) sign while using Velocity templates. If you use the dollar ($) sign, any value after it is treated as a variable. For example, if a password is configured as "$a123$q1ups$va112", the CLI Templates treats this as variables "a123", "q1ups", and "va112". To work around this issue, use the Linux shell style for text processing with Velocity templates.

- **Jinja**: Use the Jinja language. For information, see https://palletsprojects.com/projects/jinja/.

e. Choose the **Software Type** from the drop-down list.

Note You can choose the specific software type (such as IOS-XE or IOS-XR) if there are commands specific to these software types. If you choose IOS as the software type, the commands apply to all software types, including IOS-XE and IOS-XR. This value is used during provisioning to check whether the selected device confirms to the selection in the template.

In the **Device Type Details** area, do these steps:

a. Click the **Add Device Details** link.

b. Choose **Device Family** from the drop-down list.

c. Choose either the device series or device model by doing one of these tasks:

- Click the **Device Series** tab and check the check box next to the preferred device series.
- Click the **Device Models** tab and check the check box next to the preferred device model.

d. Click **Add**.

In the **Additional Details** area, do these steps:

a. Choose the **Device Tags** from the drop-down list.

Note Tags are like keywords that help you locate your template more easily.

If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get this error during provisioning:

```
Cannot select the device. Not compatible with template
```

b. Enter the **Software Version** in the software version field.

Note During provisioning, Catalyst Center checks to see if the selected device has the software version listed in the template. If there is a mismatch, the template is not provisioned.

c. Enter a **Template Description**.

Step 5 Click **Continue**.

The CLI template is created.

Note Click the **CLI Template Best Practices** link at the top-right corner of the template window to view some of the best practices that must be used in a CLI template to minimize compliance issues.

Step 6 To edit the template content, select the template that you created, click the ellipsis under **Actions**, and choose **Edit Template**. For more information, see Edit templates, on page 491.

Blocked list commands

Blocked list commands are commands that cannot be added to a template or provisioned through a template. If you use blocked list commands in your templates, it shows a warning in the template that it may potentially conflict with some of the Catalyst Center provisioning applications.

These commands are blocked in this release:

- **router lisp**
- **hostname**: This command is blocked only for routers.

Sample templates

See these sample templates for switches while creating variables for your template.

Configure snmp community

```
snmp-server community $snmp_community_name RO
```

Configure interface

```
interface $interfaceName
description $description
```

Configure NTP on Cisco Wireless Controllers

```
config time ntp interval $interval
```

Create a composite template

Two or more regular templates are grouped into a composite sequence template. You can create a composite sequential template for a set of templates, which are applied collectively to devices. For example, when you deploy a branch, you must specify the minimum configurations for the branch router. The templates that you create can be added to a single composite template, which aggregates all the individual templates that you need for the branch router. You must specify the order in which templates that are in the composite template are deployed to devices.

Note You can add only a committed template to a composite template.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 In the left pane, click **Project Name** and select the project under which you are creating templates.

Step 3 Click **Add** at the top right of the window, and choose **New Template** from the drop-down list.

The **Add New Template** slide-in pane displays.

Step 4 In the **Add New Template** slide-in pane, configure the settings for the composite template.

In the **Template Details** area, do these steps:

a) Enter a unique name in the **Template Name** field.
b) Choose the **Project Name** from the drop-down list.
c) **Template Type**: Choose **Composite Sequence** radio button.
d) Choose the **Software Type** from the drop-down list.

Note You can select the specific software type (such as IOS-XE or IOS-XR) if there are commands specific to these software types. If you select IOS as the software type, the commands apply to all software types, including IOS-XE and IOS-XR. This value is used during provisioning to check whether the selected device confirms to the selection in the template.

In the **Device Type Details** area, do these steps:

a. Click the **Add Device Details** link.

b. Choose **Device Family** from the drop-down list.

c. Choose either the device series or device model by doing one of these tasks:

- Click the **Device Series** tab and check the check box next to the preferred device series.
- Click the **Device Models** tab and check the check box next to the preferred device model.

d. Click **Add**.

In the **Additional Details** area, do these steps:

a. Choose the **Device Tags** from the drop-down list.

Note Tags are like keywords that help you locate your template more easily.

If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get this error during provisioning:

```
Cannot select the device. Not compatible with template
```

b. Enter the **Software Version** in the software version field.

Note During provisioning, Catalyst Center checks to see if the selected device has the software version listed in the template. If there is a mismatch, the template is not provisioned.

c. Enter the **Template Description**.

Step 5 Click **Continue**.
The composite template window is displayed, which shows the list of applicable templates.

Step 6 Click the **Add Templates** link, click + to add the templates, and then click **Done**.
The composite template is created.

Note Click the **CLI Template Best Practices** link at the top-right corner of the template window to view some of the best practices that must be used in a CLI template to minimize compliance issues.

Step 7 Check the check box next to the composite template that you created, click the ellipsis under **Actions** column, and choose **Commit** to commit the template content.

Edit templates

After creating a template, you can edit the template to include content.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 In the left pane, choose the **Project Name** and select the template that you want to edit.

The chosen template displays.

Note Click the **CLI Template Best Practices** link at the top-right corner of the template window to view some of the best practices that must be used in a CLI template to minimize compliance issues.

Step 3 Enter the template content. You can have a template with a single-line configuration or a multi-select configuration.

Step 4 Click **Properties** next to the template name at the top of the window to edit **Template Details**, **Device Details** and **Additional Details**. Click **Edit** next to the respective area.

Step 5 The template is auto saved. You can also choose to change the time interval of auto save, by clicking at the time recurrence next to **Auto Saved**.

Step 6 Click **Template History** to view the versions of the template. Also, you can click **Compare** to view the difference in the template versions.

Step 7 Click **Variables** tab to view the variables from the CLI template.

Step 8 Click the **Show Design Conflicts** toggle button to view potential errors in the template.

Catalyst Center allows you to view, potential and run-time errors. For more information, see Potential design conflicts detection between CLI template and service provisioning intent, on page 506 and Detect CLI template run-time conflict, on page 507.

Step 9 Click **Save** at the bottom of the window.

After saving the template, Catalyst Center checks for any errors in the template. If there are any syntax errors, the template content is not saved and all input variables that are defined in the template are automatically identified during the save process. The local variables (variables that are used in **for** loops, assigned though a set, and so on) are ignored.

Step 10 Click **Commit** to commit the template.

Note You can associate only a committed template to a network profile.

Step 11 Click **Attach to Network Profile** link, to attach the created template to a network profile.

Template simulation

The interactive template simulation lets you simulate the CLI generation of templates by specifying test data for variables before sending them to devices. You can save the test simulation results and use them later, if required.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 From the left pane, choose a project and click a template, for which you want to run a simulation.

The template displays.

Step 3 Click the **Simulation** tab.

Step 4 Click **Create Simulation**.

The **Create Simulation** slide-in pane displays.

Step 5 Enter a unique name in **Simulation Name** field.

Note If there are implicit variables in your template then select a device from the **Device** drop-down list to run the simulation against real devices based on your bindings.

Step 6 Click **Import Template Parameters** to import the template parameters or click **Export Template Parameters** to export the template parameters.

Step 7 To use the variables from the last device provisioning, click **Use Variable Values from the Last Provisioning** link. New variables must be added manually.

Step 8 Choose values of the variables, by clicking on the link and click **Run**.

Export templates

You can export a template or multiple templates to a single file, in JSON format.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 Check a check box or multiple check box, next to the template name to select a template or multiple template that you want to export.

Step 3 From the **Export** drop-down list, choose **Export Template**.

Step 4 (Optional) You can filter the templates based on categories in the left pane.

Step 5 The latest version of the template is exported.

To export an earlier version of the template, do these steps

a. Click the template name to open the template.

b. Click **Template History** tab.

The **Template History** slide-in pane displays.

c. Choose the preferred version.

d. Click **View** button below the version.

The CLI template of that version displays.

e. Click **Export** at the top of the template.

The JSON format of the template is exported.

Import templates

You can import a template or multiple templates under a project.



Note You can import templates only from an earlier version of Catalyst Center to a newer version. However, the opposite is not allowed.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 In the left pane, choose the project for which you want to import templates, under **Project Name** and choose **Import** > **Import Template**.

Step 3 **Import Templates** slide-in pane displays.

a. Choose the **Project Name** from the drop-down list.

b. Upload the JSON file by doing one of these actions:

1. Drag and drop the file to the drag and drop area.
2. Click, **Choose a file**, browse to the location of the JSON file, and click **Open**.

File size should not exceed 10Mb.

c. Check the check box to create a new version of imported template, if template with the same name already exists in the hierarchy.

d. Click **Import**.

The CLI template is successfully imported to the chosen project.

Clone a template

You can make a copy of a template to reuse portions of it.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 Click the ellipsis under **Action** column and choose **Clone**.

Step 3 The **Clone Template** slide-in pane displays.

Do these steps:

a. Enter a unique name in **Template Name** field.

b. Choose the **Project Name** from the drop-down list.

Step 4 Click **Clone**.

The latest version of the template is cloned.

Step 5 (Optional) Alternatively, you can clone the template by clicking the template name. The template is displayed. Click **Clone** above the template.

Step 6 To clone an earlier version of the template, do these steps:

a. Select the template by clicking the template name.

b. Click the **Template History** tab.

The **Template History** slide-in pane displays.

c. Click the preferred version.

The chosen CLI template displays.

d. Click **Clone** above the template.

Attach a CLI template to the network profiles

Use this procedure to attach a CLI template to a network profile or multiple network profiles.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

The **CLI Templates** window is displayed.

Step 2 In the **Templates** table, under **Network Profile** column, click **Attach** to attach a template to the network profile.

Note Alternatively, you can click the ellipsis under **Actions** column and choose **Attach to Profile**, or you can attach a template to the network profile from **Design** > **Network Profiles** window. For more information, see Associate templates to network profiles, on page 504.

The **Attach to Network Profile** slide-in pane displays.

Step 3 Check the check box next to the network profile name and click **Save**.
The CLI template is attached to the chosen network profile.

Step 4 The number displayed under **Network Profile** column shows the number of network profiles attached to a CLI template. Click the number to view the network profile details.

Step 5 To attach more network profiles to a CLI template, do these steps:

a. Click the number under **Network Profile** column.

Alternatively, in **Actions** column, click the ellipsis icon and choose **Attach to Profile**.

The **Network Profiles** slide-in pane displays.

b. Click **Attach to Network Profile** link at the top right of the slide-in pane, check the check box next to the network profile name, and click **Attach**.

Provision CLI templates

You can provision a CLI template by attaching a network profile to the template or by not associating the template with a network profile.

If you want to configure one or a few devices with specific configurations that do not apply to the rest of the devices at the same site, you can provision the CLI template without associating it with a network profile. The compliance check is skipped if you provision the template without associating it with a network profile.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 Check the check box next to the template that you want to provision and click **Provision Templates** at the top of the table.

You can provision multiple templates.

If you have not attached a network profile to the template, a warning message appears. Click **Yes** in the warning message to provision the template without a network profile.

You are redirected to the **Provision Template** workflow.

Step 3 In the **Get Started** window, enter a unique name in the **Task Name** field.

Step 4 In the **Select Devices** window, choose the devices from the applicable devices list, which are based on the device details defined in the template. Click **Next**.

Step 5 In the **Review Applicable Templates** window, review the devices and the attached templates. If required, you can remove the templates that you do not want to be provisioned on the device.

Step 6 In the **Configure Template Variables** window, configure the template variables for each device.

Step 7 In the **Preview Configuration** window, select the device to preview the configuration that is being provisioned on it.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

If the provisioning of a template fails, Catalyst Center does not attempt to roll back the commands that were pushed before the template provisioning failure.

Export projects

You can export a project or multiple projects, including their templates, to a single file in JSON format.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 In the left pane, select a project or multiple project that you want to export under **Project Name**.

Step 3 From **Export** drop-down list, choose **Export Project**.

Step 4 Click **Save**, if prompted.

Import projects

You can import a project or multiple projects with their templates, into the Catalyst Center **CLI Templates**.

Note You can import projects only from an earlier version of Catalyst Center to a newer version. However, the opposite is not allowed.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 From the **Import** drop-down list, choose **Import Project**.

Step 3 The **Import Projects** slide-in pane displays.

a. Upload the JSON file by doing one of these actions:

1. Drag and drop the file to the drag and drop area.
2. Click **Choose a file**, browse to the location of the JSON file, and click **Open**.

File size should not exceed 10Mb.

b. Check the check box to create a new version of the template in the existing project, if the project with the same name is already in the hierarchy.

c. Click **Import**.

The project is successfully imported.

Template variables

The template variables are used for adding additional metadata information in the template. You can also use the variables to provide validations for variables such as maximum length, range, and so on.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 From the left pane, choose a project and click a template.

The template displays.

Step 3 Click the **Variables** tab.

It enables you to add metadata to the template variables. All the variables that are identified in the template display. You can configure the these metadata:

- Choose the variable from the left pane, and click the **Variable** toggle button if you want the string to be considered as a variable.

  Note By default the string considered as a variable. Click the toggle button, if you do not want the string to be considered as a variable.

- Check the **Required Variable** check box if this is a required variable during the provisioning. All the variables by default are marked as Required, which means you must enter the value for this variable at the time of provisioning. If the parameter is not marked as **Required Variable** and if you do not pass any value to the parameter, it substitutes an empty string at run time. A lack of a variable can lead to command failure, which may not be syntactically correct. If you want to make an entire command optional based on a variable not marked as **Required Variable**, use the **if-else** block in the template.
- Enter the field name in the **Field Name**. This is the label that is used for the UI widget of each variable during provisioning.
- In **Variable Data Value** area, choose the **Variable Data Source** by clicking the radio button. You can choose, **User Defined** value or **Bound to Source** value to hold a specific value.

  Do these steps, if you choose **User Defined** value:

  a. Choose the **Variable Type** from the drop-down list: **String**, **Integer**, **IP Address**, or **Mac Address**

  b. Choose the **Data Entry Type** from the drop-down list: **Text Field**, **Single Select**, or **Multi Select**.

  c. Enter the default variable value in the **Default Variable Value** field.

  d. Check the **Sensitive Value** check box for sensitive value.

  e. Enter the number of characters that are allowed in the **Maximum Characters** field. This is applicable only for the string data type.

  f. Enter hint text in the **Hint Text** field.

  g. Enter any additional information in the **Additional Info** text box.

  Do these steps, if you choose **Bound to Source** value:

  a. Choose the **Data Entry Type** from the drop-down list: **Text Field**, **Single Select**, or **Multi Select**.

  b. Choose the **Source** from the drop-down list: **Network Profile**, **Common Settings**, **Cloud Connect** and **Inventory**.

  c. Choose the **Entity** from the drop-down list.

  d. Choose the **Attribute** from the drop-down list.

  e. Enter the number of characters that are allowed in the **Maximum Characters** field. This is applicable only for the string data type.

f. Enter hint text in the **Hint Text** field.

g. Enter any additional information in the **Additional Info** text box.

For more details on **Bound to Source** value, see Variable binding, on page 499.

Step 4 After configuring metadata information, click **Review Form** to review the variable information.

Step 5 Click **Save**.

Step 6 To commit the template, choose **Commit**. The **Commit** window displays. You can enter a commit note in the **Commit Note** text box.

Variable binding

While creating a template, you can specify variables that are contextually substituted. Many of these variables are available under **Design** > **CLI Templates**.

CLI templates provide an option to bind or use variables in the template with the source object values while editing or through the input form enhancements; for example, DHCP server, DNS server, and syslog server.

Some variables are always bound to their corresponding source and their behavior cannot be changed. To view the list of implicit variables, click the template and click **Variables** tab.

Note Variable binding is not supported for the day-zero template, it is only supported for the day-n template.

The predefined object values can be one of these values:

- Network Profile:
  - SSID
  - Policy profile
  - AP group
  - Flex group
  - Flex profile
  - Site tag
  - Policy tag
- Common Settings:
  - DHCP server
  - Syslog server
  - SNMP trap receiver
  - NTP server
  - Timezone site

- Device banner
- DNS server
- NetFlow collector
- AAA network server
- AAA endpoint server
- AAA server pan network
- AAA server pan endpoint
- WLAN info
- RF profile info

- Cloud Connect:
  - Cloud router-1 Tunnel IP
  - Cloud router-2 Tunnel IP
  - Cloud router-1 Loopback IP
  - Cloud router-2 Loopback IP
  - Branch router-1 Tunnel IP
  - Branch router-2 Tunnel IP
  - Cloud router-1 Public IP
  - Cloud router-2 Public IP
  - Branch router-1 IP
  - Branch router-2 IP
  - Private subnet-1 IP
  - Private subnet-2 IP
  - Private subnet-1 IP mask
  - Private subnet-2 IP mask

- Inventory:
  - Device
  - Interface
  - AP group
  - Flex group
  - WLAN
  - Policy profile

- Flex profile
- Webauth parameter map
- Site tag
- Policy tag
- RF profile

- **Common Settings**: Settings available under **Design** > **Network Settings** > **Network**. The common settings variable binding resolves values that are based on the site to which the device belongs.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

Step 2 Choose the template and click the **Variables** tab to bind variables in the template to network settings.

Step 3 Select the variables in the left pane and check the **Required Variable** check box to bind variables to the network settings.

Step 4 To bind variables to network settings, select each variable from the left pane, and under **Variable Data Source**, click the **Bound to Source** radio button. Do these steps:

a. From the **Data Entry Type** drop-down list, choose the type of UI widget to create at the time of provisioning: **Text Field**, **Single Select**, or **Multi Select**.

b. Choose the **Source**, **Entity**, and **Attribute** from the respective drop-down lists.

c. For the source type **CommonSettings**, choose one of these entities: **dhcp.server**, **syslog.server**, **snmp.trap.receiver**, **ntp.server**, **timezone.site**, **device.banner**, **dns.server**, **netflow.collector**, **aaa.network.server**, **aaa.endpoint.server**, **aaa.server.pan.network**, **aaa.server.pan.endpoint**, **wlan.info** or **rfprofile.info**.

You can apply a filter on the **dns.server** or **netflow.collector** attributes to display only the relevant list of **bind** variables during provisioning of devices. To apply a filter on an attribute, select an attribute from the **Filter by** drop-down list. From the **Condition** drop-down list, select a condition to match the **Value**.

d. For the source type **NetworkProfile**, choose **SSID** as the entity type. The SSID entity that is populated is defined under **Design** > **Network Profile**. The binding generates a user-friendly SSID name, which is a combination of SSID name, site, and SSID category. From the **Attributes** drop-down list, choose **wlanid** or **wlanProfileName**. This attribute is used during the advanced CLI configurations at the time of template provisioning.

e. For the source type **Inventory**, choose one of these entities: **Device**, **Interface**, **AP Group**, **Flex Group**, **Wlan**, **Policy Profile**, **Flex Profile**, **Webauth Parameter Map**, **Site Tag**, **Policy Tag**, or **RF Profile**. For the entity type **Device** and **Interface**, the **Attribute** drop-down list shows the device or interface attributes. The variable resolves to the AP Group and Flex Group name that is configured on the device to which the template is applied.

You can apply filter on the **Device**, **Interface**, or **Wlan** attributes to display only the relevant list of **bind** variables during provisioning of devices. To apply a filter on an attribute, select an attribute from the **Filter by** drop-down list. From the **Condition** drop-down list, select a condition to match the **Value**.

After binding variables to a common setting, when you assign templates to a wireless profile and provision the template, the network settings that you defined under **Network Settings** > **Network** appear in the drop-down list. You must define these attributes under **Network Settings** > **Network** at the time of designing your network.

Step 5 If the template contains variable bindings that bind to specific attributes and the template code accesses those attributes directly, you must do one of these tasks:

- Change the binding to the object instead of to the attributes.
- Update the template code to not access the attributes directly.

For example, if the template code is as follows, where **$interfaces** binds to specific attributes, you must update the code as shown in these examples, or modify the binding to the object instead of to the attributes.

Old sample code:

```
#foreach ( $interface in $interfaces )
 $interface.portName
      description "something"
#end
```

New sample code:

```
#foreach ( $interface in $interfaces )
 interface $interface
           description "something"
#end
```

Special keywords

All commands executed through templates are always in the **config t** mode. Therefore, you do not have to specify the **enable or config t** commands explicitly in the template.

Day-zero templates do not support special keywords.

Enable Mode commands

Specify the **#MODE_ENABLE** command if you want to execute any commands outside of the **config t** command.

Use this syntax to add **enable mode** commands to your CLI templates:

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

Interactive commands

Specify **#INTERACTIVE** if you want to execute a command where a user input is required.

An interactive command contains the input that you must enter the execution of a command. To enter an interactive command in the CLI Content area, use this syntax:

```
CLI Command<IQ>interactive question 1 <R> command response 1 <IQ>interactive question
2<R>command response 2
```

Where **<IQ>** and **<R>** tags evaluate the text provided against what is seen on the device.

The Interactive question uses regular expressions to validate if the text received from the device is similar to the text entered. If the regular expressions entered in the **<IQ><R>** tags are found, then the interactive question passes and a part of the output text appears. This means that you need to enter a part of the question and not the entire question. Entering Yes or No between the **<IQ>** and **<R>** tags is sufficient but you must make sure that the text Yes or No appears in the question output from the device. The best way to do this is by running

the command on the device and observing the output. In addition, you need to ensure that any regular expression metacharacters or newlines entered are used appropriately or avoided completely. The common regular expression metacharacters are **. ( ) [ ] { } | * + ? \ $ ^ : &**.

For example, this command has output that includes metacharacters and newlines:

```
Switch(config)# no crypto pki trustpoint server-CA
% Removing an enrolled trustpoint will destroy all certificates received from the related
Certificate Authority
Are you sure you want to do this? [yes/no]:
```

To enter this in a template, you need to select a portion that does not have any metacharacters or newlines. Here are a few examples of what can be used:

```
#INTERACTIVE
no crypto pki trustpoint server-CA<IQ>yes/no<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint server-CA<IQ>Removing an enrolled<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint server-CA<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Where **<IQ>** and **<R>** tags are case-sensitive and must be entered in uppercase.

Note In response to the interactive question after providing a response, if the newline character is not required, you must enter the **<SF>** tag. Include one space before the **<SF>** tag. When you enter the **<SF>** tag, the **</SF>** tag pops up automatically. You can delete the **</SF>** tag because it is not needed.

For example:

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#ENDS_INTERACTIVE
```

Combining interactive Enable Mode commands

Use this syntax to combine interactive **Enable Mode** commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
#ENDS_INTERACTIVE
#MODE_END_ENABLE

#MODE_ENABLE
#INTERACTIVE
```

```
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Multiline commands

If you want multiple lines in the CLI template to wrap, use the **MLTCMD** tags. Otherwise, the command is sent line by line to the device. To enter multiline commands in the CLI Content area, use this syntax:

```
<MLTCMD>first line of multiline command
second line of multiline command
...
...
last line of multiline command</MLTCMD>
```

- Where **<MLTCMD>** and **</MLTCMD>** are case-sensitive and must be in uppercase.
- The multiline commands must be inserted between the **<MLTCMD>** and **</MLTCMD>** tags.
- The tags cannot start with a space.
- The **<MLTCMD>** and **</MLTCMD>** tags cannot be used in a single line.

Associate templates to network profiles

Before you begin

Before provisioning a template, ensure that the template is associated with a network profile and the profile is assigned to a site.

During provisioning, when the devices are assigned to specific sites, the templates associated with the site through the network profile appear in the advanced configuration.

Procedure

Step 1 From the main menu, choose **Design** > **Network Profiles**, and click **Add Profile**.

Profile types available, include:

- **Assurance**: Click this to create an Assurance profile.
- **Firewall**: Click this to create a firewall profile.
- **Routing**: Click this to create a routing profile.
- **Switching**: Click this to create a switching profile.
  - Click the **Onboarding Templates** or **Day-N Templates**, as required.
  - In the **Profile Name** field, enter the profile name.
  - Click **+Add Template** and choose the device type, tag, and template from the **Device Type**, **Tag Name**, and **Template** drop-down lists.

    If you do not see the template that you need, create a new template in **Design** > **CLI Templates** window. For more information, see Create a regular template, on page 487.

- Click **Save**.

- **Telemetry Appliance**: Click this to create a Catalyst Center Traffic Telemetry Appliance profile.
- **Wireless**: Click this to create a wireless profile. Before assigning a wireless network profile to a template, ensure that you have created wireless SSIDs.
  - In the **Profile Name** field, enter the profile name.
  - Click **+ Add SSID**. The SSIDs that were created under **Network Settings** > **Wireless** are populated.
  - Under **Attach Template(s)**, from the **Template** drop-down list, choose the template that you want to provision.
  - Click **Save**.



Note You can view the Switching and Wireless profiles in the **Cards** and the **Table** view.

Step 2 The **Network Profiles** window lists these values:

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- **Sites**: Click **Assign Site** to add sites to the selected profile.

Step 3 For day-*n* provisioning, choose **Provision** > **Network Devices** > **Inventory** and do these steps:

a) Check the check box next to the device name that you want to provision.
b) From the **Actions** drop-down list, choose **Provision**.
c) In the **Assign Site** window, assign a site to which the profiles are attached.
d) In the **Choose a Site** field, enter the name of the site to which you want to associate the controller, or choose from the **Choose a Site** drop-down list.
e) Click **Next**.
f) The **Configuration** window appears. In the **Managed AP Locations** field, enter the AP locations managed by the controller. You can change, remove, or reassign the site. This is applicable only for wireless profiles.
g) Click **Next**.
h) The **Advanced Configuration** window appears. The templates associated with the site through the network profile appear in the advanced configuration.
   - Check the **Provision these templates even if they have been deployed before** check box if you overwrote any configurations from intent in the template, and you want your changes to override. (This option is disabled by default.)
   - The **Copy running config to startup config** option is enabled by default, which means that after deploying the template configuration, **write mem** will be applied. If you don't want to apply the running config to the startup config, you must uncheck this check box.
   - Use the **Find** feature to quickly search for the device by entering the device name, or expand the templates folder and select the template in the left pane. In the right pane, select values for those attributes that are bound to the source.

- To export the template variables into a CSV file while deploying the template, click **Export** in the right pane. You can use the CSV file to make necessary changes in the variable configuration and import it into Catalyst Center at a later time by clicking **Import** in the right pane.

i) Click **Next** to deploy the template.
j) Choose whether you want to deploy the template **Now** or schedule it for later.
The **Status** column in the **Device Inventory** window shows SUCCESS after the deployment succeeds.

Step 4 Click **Export Deployment CSV** to export template variables from all the templates in a single file.

Step 5 Click **Import Deployment CSV** to import template variables from all the templates in a single file.

Step 6 For day-zero provisioning, choose **Provision** > **Plug and Play** and do these steps:

a) Choose a device from the **Actions** drop-down list, and choose **Claim**.
b) Click **Next** and in **Site Assignment** window, choose a site from the **Site** drop-down list.
c) Click **Next** and in **Configuration** window, choose the image and the day-zero template.
d) Click **Next** and in the **Advanced Configuration** window, enter the location.
e) Click **Next** to view the **Device Details**, **Image Details**, **Day-0 Configuration Preview**, and **Template CLI Preview**.

Detect conflicts in a CLI template

Catalyst Center allows you to detect conflicts in a CLI template. You can view potential design conflicts and run-time conflicts for switching, wireless, SD-Access, or fabric.

Potential design conflicts detection between CLI template and service provisioning intent

Potential design conflicts identify the intent commands in the CLI template and flag them, if the same command is pushed by switching, wireless, SD-Access, or fabric. Intent commands are not recommended for use, because Catalyst Center supports this configuration through intent provision for device.

Procedure

Step 1 From the main menu, choose **Design** > **CLI Templates**.

The **CLI Templates** window displays.

Step 2 (Optional) In the left pane, from the **Project Name** drop-down list, choose a project with your preferred CLI templates.



Note To view only the templates with conflicts, in the left pane, under **Potential Design Conflicts**, check the **Conflicts** check box.

Step 3 Click the template name to view the total number of conflicts.

Alternatively, under the **Potential Design Conflicts** column, you can also view the total number of conflicts by clicking the warning icon.

The CLI Template is displayed.

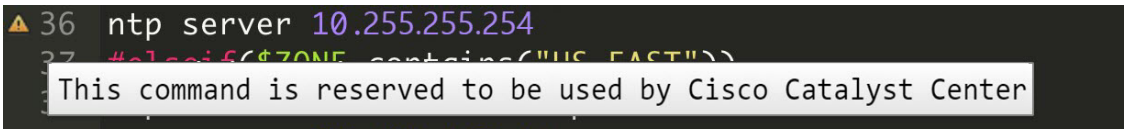
Step 4 To show the conflicts, click the **Show Design Conflicts** toggle button.

Step 5 In the template, hover your cursor over the warning icon to view the details of the conflict.

The CLI commands that have conflicts are flagged with a warning icon. For new templates, the conflicts are detected after you save the template.

Example:

When the intent command **ntp server** is used in the CLI template, Catalyst Center displays this message when you hover your cursor over the warning icon:



Step 6 (Optional) You can also view the number of conflicts on newly configured CLI templates by doing these steps:

a) From the main menu, choose **Provision** > **Inventory**.

On the **Inventory** window, a message with a warning icon displays, which shows the number of conflicts in the newly configured CLI template.

b) Click the **Update CLI Templates** link to view the conflicts.

Detect CLI template run-time conflict

Run-time conflict detection matches the exact CLI commands in the CLI template with the already provisioned commands. If an exact command match is detected, Catalyst Center flags the command. Catalyst Center allows you to detect run-time conflict for switching, wireless, SD-Access, or fabric.

Note Catalyst Center doesn't support run-time conflict detection for Cisco Catalyst 9800 Series Wireless Controllers.

Before you begin

You must configure the CLI template through Catalyst Center to detect run-time conflict.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays.

Step 2 Under the **Template Provision Status** column, view the template provisioning status of devices, which shows the number of templates provisioned on the device.

The templates that are provisioned successfully display with a tick icon. The templates that have conflicts display with a warning icon.

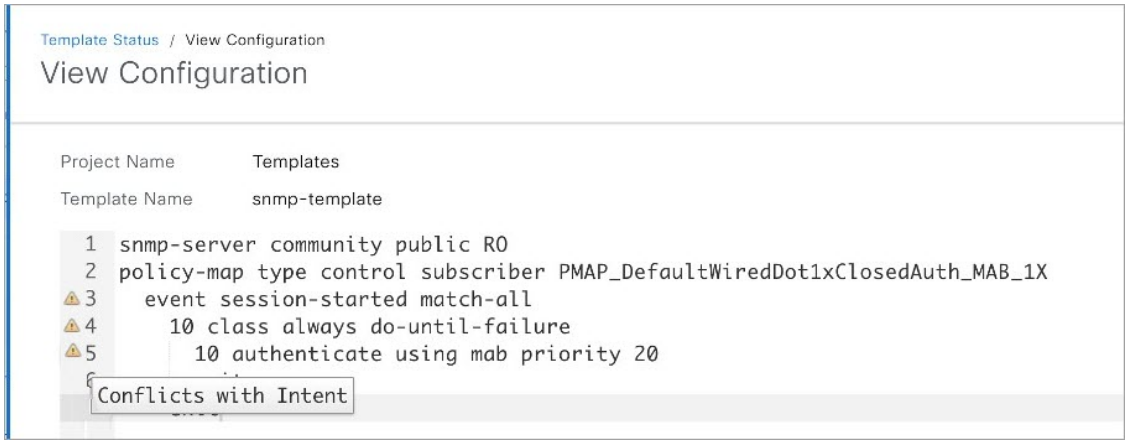
Step 3 Under the **Template Provision Status** column, click the link to open the **Template Status** slide-in pane.

You can view this information in the table:

- **Template Name**
- **Project Name**
- **Provision Status**: Displays **Template Provisioned** if the template was provisioned successfully or **Template Out of Sync** if there are any conflicts in the template.
- **Conflict Status**: Displays the number of conflicts in the CLI template.
- **Actions**: Click **View Configuration** to view the CLI template. Commands that have conflicts are flagged with a warning icon.

Example:

This example shows the **View Configuration** slide-in pane with run-time conflicts:



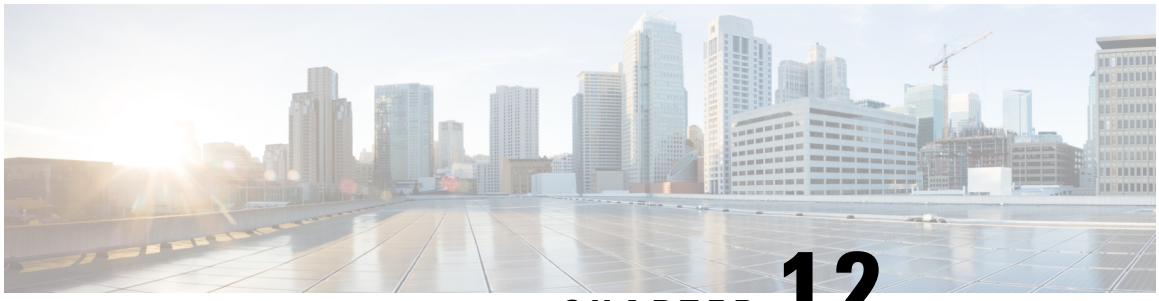
Step 4 (Optional) You can view the number of conflicts in a CLI template under the **Template Conflicts Status** column in the **Inventory** window.

Step 5 Identify the run-time conflicts by generating a configuration preview:

a) Check the check box next to the device name.
b) From the **Actions** drop-down list, choose **Provision Device**.
c) On the **Assign Site** window, click **Next**. On the **Advanced Configuration** window, make the necessary changes and click **Next**. On the **Summary** window, click **Deploy**.
d) In the **Provision Device** slide-in pane, click the **Generate Configuration Preview** radio button and click **Apply**.
e) Click the **Work Items** link to view the generated configuration preview.

   Alternatively, click the menu icon and choose **Activities** > **Tasks** and open the work item to view the generated configuration preview.

f) (Optional) If the activity is still loading, click **Refresh**.
g) Click the preview link to open the **Configuration Preview** slide-in pane. You can view the CLI commands with run-time conflicts that are flagged with warning icons.



CHAPTER 12

Design Feature Templates

- Introduction to feature templates, on page 509
- Discover and create designs from a legacy device, on page 510
- Create a feature template for AAA RADIUS attributes, on page 511
- Create a feature template for advanced SSID, on page 512
- Create a feature template for Cisco CleanAir, on page 517
- Create a feature template for Dot11ax configuration, on page 519
- Create a feature template for Dot 11be status configuration, on page 521
- Create a feature template for event-driven RRM configuration, on page 522
- Create a feature template for Flex configuration, on page 524
- Create a feature template for Global IPv6 Configuration, on page 525
- Create a feature template for Multicast, on page 526
- Create a feature template for RRM FRA parameters, on page 527
- Create a feature template for RRM general parameters, on page 528
- Create a feature template for rogue general parameters, on page 530

Introduction to feature templates

Feature templates (previously known as model configurations) allow you to define advanced customizations of the Cisco Validated Designs (CVDs) that are encapsulated within the provisioning applications. Feature templates are a set of model-based, discoverable, and customizable configuration capabilities, which you can deploy on your network devices with high-level service intent and device-specific CLI templates.

Feature templates simplify network provision by extracting complex device configurations and facilitating customizable network configurations using an intuitive GUI instead of device-specific CLIs. A common design is deployed to various device hardware platforms and software types in a uniform way. During deployments, the Catalyst Center infrastructure automatically validates and translates extracted designs to device-specific CLI commands.

To provision feature templates:

1. Create a feature template on the **Design** > **Feature Templates** window.
2. Apply the feature template to different network profiles.
3. Using the provision workflow, apply the feature template that is specified in network profiles to a network device.

Note When a CLI template is in use, wait for the inventory sync to complete before provisioning to apply the feature template configurations.

Supported feature templates

Catalyst Center supports wireless feature templates, including:

- AAA Radius attributes configuration
- Advanced SSID configuration
- CleanAir configuration
- Dot11ax configuration
- Dot11be status configuration
- Event driven RRM configuration
- Flex configuration
- Global IPv6 configuration
- Multicast configuration
- RRM FRA configuration
- RRM general configuration
- Rogue general configuration

Discover and create designs from a legacy device

Instead of manually creating designs using **Feature Templates**, you can use the **Discover Feature Templates** feature to discover the existing feature templates available on legacy devices and use them as a template to create new feature templates.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 Click the **Discovery** tab.

A list of discovered devices that are available in the **Inventory** window displays.

Step 3 Click the radio button next to the device name and click **Discover Feature Templates**.

Step 4 In the right pane, expand **Wireless** and choose a feature template.

The configuration available for the selected feature template is displayed. For example, if you choose **CleanAir Configuration** under **Wireless**, the available feature template for the CleanAir configuration displays.

Step 5 Check the check box next to the feature templates that you want to use as a template to create a new design, and click **Create Design**.

Step 6 In the window that displays, make the necessary changes and click **Save**.

Create a feature template for AAA RADIUS attributes

Use the **AAA Radius Attributes Configuration** feature template to define the Called-station-id parameter value for Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

The **Default AAA Radius Attributes Configuration** defines the called-station ID as **ap-macaddress-ssid**. You can't edit or delete this default feature template. However, you can create a custom feature template for your specific network design.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **AAA Radius Attributes Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Called-station-id** slide-in pane, enter a name for the feature template.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 From the **Called-station-id** drop-down list, choose an attribute value.

Step 7 Click **Save**.

The new design instance displays in the **Design Instances** window.

Step 8 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can deploy on a wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.

2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620 or Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Create a feature template for advanced SSID

A WLAN associates a service set identifier (SSID) to an interface or an interface group. The WLAN is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. You can configure up to 512 WLANs for each wireless controller.

Use the **Advanced SSID Configuration** feature template to configure the advanced SSID parameters on devices. **Default Advanced SSID Design** is the default advanced SSID feature template. You can't edit or delete the default design. However, you can create a custom feature template for your specific network design.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Advanced SSID Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Advanced SSID Configuration** slide-in pane, enter a name for the feature template.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 In the **General** tab, do these steps:

a) From the **Peer to Peer Blocking** drop-down list, choose an option for peer-to-peer blocking.

Peer-to-peer blocking is applied to individual WLANs. Each client inherits the peer-to-peer blocking setting of the WLAN to which it's associated. Peer-to-peer blocking enables you to have more control over how traffic is directed.

- **DISABLE**: Disables peer-to-peer blocking and forwards traffic locally within the wireless controller whenever possible.
- **DROP**: Causes the wireless controller to discard the client packets.
- **FORWARD UP**: Causes the client packets to be forwarded on an upstream VLAN. The device above the wireless controller decides what to do with the packets. The device can either be a router or a Layer 3 switch.
- **ALLOW PVT GROUP**: Applicable to preshared key (PSK) clients only. Traffic is forwarded based on the associated identity PSK (IPSK) tags for the source and destination client devices.

b) Click the **Passive Client Enable** toggle button to enable the Passive Client feature.

Passive clients are wireless devices, such as scales and printers, that are configured with a static IP address. These clients don't transmit any IP information (such as IP address, subnet mask, and gateway information) when they associate with an AP. As a result, when passive clients are used, the wireless controller never knows the IP address unless they use DHCP.

c) Click the **Assisted Roaming Prediction Optimization** toggle button to configure an assisted roaming prediction list for a WLAN.

d) Click the **Neighbor List Dual Band** toggle button to configure a neighbor list on a dual radio band.

e) Click the **Network Admission Control (NAC-SNMP)** toggle button to enable SNMP NAC support on the WLAN.

f) Click the **Network Admission Control (NAC-Radius)** toggle button to enable RADIUS NAC support on the WLAN.

g) From the **DHCP Required** drop-down list, choose **Yes** or **No** to pass the DHCP request before going into the RUN state (a state where the client can pass traffic through the wireless controller).

h) In the **DHCP Server - IP Address** field, enter the IP address of the DHCP server.

i) Click the **FlexConnect Local Authentication** toggle button to enable FlexConnect local authentication.

j) Click the **802.11ax Status** toggle button to enable 802.11ax configuration parameters.

k) Click the **Aironet IE** toggle button to enable support for Aironet IE on this SSID.

l) Click the **Load Balance Enable** toggle button to enable the load balancing feature.

m) In the **DTIM Period 5GHz Band (In Beacon Intervals) [1-255]** field, enter a value for the 5-GHz band.

The valid range is from 1 to 255. The default value is 1 (to transmit broadcast and multicast frames after every beacon).

If the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the AP transmits buffered broadcast and multicast frames 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the AP transmits buffered broadcast and multicast frames five times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon).

n) In the **DTIM Period 2.4GHz Band (In Beacon Intervals) [1-255]** field, enter a value for the 2.4-GHz band. The valid range is from 1 to 255. The default value is 1 (to transmit broadcast and multicast frames after every beacon).

o) In the **Max Clients Per WLAN** field, enter the maximum number of clients that are allowed to join the WLAN.

The valid range is from 0 to 10,000.

p) In the **Max Clients Per AP Radio Per WLAN [0-500]** field, enter the maximum number of clients that are allowed to join the WLAN per AP.

The valid range is from 0 to 500.

q) In the **Max Clients Per AP Per WLAN [0-1200]** field, enter the maximum number of client connections that are allowed per AP.

The valid range is from 0 to 1200.

r) From the **WMM Policy** drop-down list, choose an option for the WMM policy: **Allowed**, **Disabled**, or **Required**.

By default, the WMM policy is **Allowed**.

s) In the **NAS ID** field, enter the network access server identifier.

Step 7 In the **Client Data Rates** tab, configure these client data rate limits per client by entering values in the respective fields:

- **Average Downstream Data Rate Per Client (kbps)**
- **Burst Downstream Data Rate Per Client (kbps)**
- **Average Downstream Real-Time Rate Per Client (kbps)**
- **Burst Downstream Real-Time Rate Per Client (kbps)**
- **Average Upstream Data Rate Per Client (kbps)**
- **Burst Upstream Data Rate Per Client (kbps)**
- **Average Upstream Real-Time Rate Per Client (kbps)**
- **Burst Upstream Real-Time Rate Per Client (kbps)**

Step 8 In the **SSID Data Rates** tab, configure these SSID data rate limits per SSID by entering values in the respective fields:

- **Average Upstream Data Rate Per SSID (kbps)**
- **Burst Upstream Data Rate Per SSID (kbps)**
- **Average Upstream Real-Time Rate Per SSID (kbps)**
- **Burst Upstream Real-Time Rate Per SSID (kbps)**
- **Average Downstream Data Rate Per SSID (kbps)**
- **Burst Downstream Data Rate Per SSID (kbps)**
- **Average Downstream Real-Time Rate Per SSID (kbps)**
- **Burst Downstream Real-Time Rate Per SSID (kbps)**

Step 9 Hover your cursor over **More** and click **802.11ax Configuration** to configure the 802.11ax BSS configuration parameters. To enable or disable these parameters, you can use the corresponding toggle buttons:

- **BSS Target Wake Up Time**
- **Downlink OFDMA**
- **Uplink OFDMA**
- **Downlink MU-MIMO**
- **Uplink MU-MIMO**

Note These parameters apply only to 2.4-GHz and 5-GHz radio bands. You can configure 802.11ax parameters for the 6-GHz radio band under the **Design** > **Network Settings** > **Wireless** > **RF Profiles** window. For more information, see Create a wireless radio frequency profile, on page 383.

Starting with Cisco IOS XE Release 17.18.2, the **OFDMA Uplink**, **OFDMA Downlink**, **MU-MIMO Uplink**, and **MU-MIMO Downlink** parameters are also used for the corresponding 802.11be configurations on the 2.4-GHz and 5-GHz radio bands.

Step 10 Hover your cursor over **More** and click **Off Channel Scanning Defer** to configure the scan defer time and defer priority.

a) In the **Scan Defer Time [0-60000msecs]** field, set the time in milliseconds.

The valid range is from 0 to 60,000 milliseconds; the default value is 100 milliseconds. If you set the time to 0, the scan deferral doesn't happen. The scan defer time is common for all priorities on the same WLAN, and the scan is deferred if a packet is transmitted or received in any one of the deferred priorities.

b) Click the corresponding toggle buttons to configure the required priority markings for packets:

- **Defer Priority0**
- **Defer Priority1**
- **Defer Priority2**
- **Defer Priority3**
- **Defer Priority4**
- **Defer Priority5**
- **Defer Priority6**
- **Defer Priority7**

Note These parameters aren't supported on the Cisco AireOS Wireless Controller.

Step 11 Hover your cursor over **More** and click **Device Analytics** to configure the device analytics parameters:

a) Click the **Share Data with Client** toggle button to enable sharing Cisco device data with the client.
b) Click the **Advertise Support** toggle button to configure device analytics support.
c) Click the **Advertise PC Analytics Support** toggle button to configure PC analytics support.

Note These parameters aren't supported on the Cisco AireOS Wireless Controller.

Step 12 Hover your cursor over **More** and click **802.11k Beacon Radio Measurement** to configure the 802.11k beacon radio measurement parameters:

a) Click the **Client Scan Report On Association** toggle button to send beacon measurement request (client scan report) on client association.
b) Click the **Client Scan Report On Roam** toggle button to send a beacon measurement request (client scan report) on client roaming.

Note These parameters aren't supported on the Cisco AireOS Wireless Controller.

Step 13 Hover your cursor over **More** and click **Multicast Buffer** to configure the multicast buffer parameter:

a) Click the **Multicast Buffer Enable** toggle button to configure multicast buffer tuning mode for 802.11a radio for WLAN.



Note This parameter isn't supported on the Cisco AireOS Wireless Controller.

Step 14 Hover your cursor over **More** and click **SIP-CAC** to configure the SIP Call Admission Control (CAC) parameters:

a) Click the **Call Snooping** toggle button to configure call snooping for the WLAN mapped to the policy profile.
b) Click the **Send Disassociate** toggle button to configure the SIP CAC send disassociate option.
c) Click the **Send 486 Busy** toggle button to configure the SIP CAC send 486 busy option.



Note These parameters aren't supported on the Cisco AireOS Wireless Controller.

Step 15 Hover your cursor over **More** and click **Miscellaneous** to configure these parameters:

a) Click the **Media Stream Multicast-Direct** toggle button to configure multicast direct for WLAN.
b) Click the **802.11ac MU-MIMO** toggle button to configure 802.11ac MU-MIMO on WLAN.
c) Click the **Wifi To Cellular Steering** toggle button to configure Wi-Fi to cellular steering on WLAN.
d) Click the **Wi-Fi Alliance Agile Multiband** toggle button to configure Wi-Fi alliance agile multiband (MBO) support.
e) Click the **Fastlane+ (ASR)** toggle button to configure advanced scheduling request handling on WLAN.
f) Click the **Dot11v Bss Max Idle Protected** toggle button to configure BSS maximum idle processing per WLAN.
g) Click the **Universal Admin** toggle button to allow universal admin mode to be enabled on a 802.1x, WPA, or WPA2-secured WLAN.
h) Click the **Opportunistic Key Caching** toggle button to configure opportunistic key caching.
i) Click the **IP Source Guard** toggle button to configure MAC verification.
j) Click the **Enable DHCP Option82 Remote ID suboption** toggle button to configure the DHCP Option82 remote ID option.
k) Click the **VLAN Central Switching** toggle button to configure VLAN central switching.
l) Click the **IP Mac Binding** toggle button to configure control over support for IP MAC binding creation.
m) In the **Idle threshold (0-4294967295 bytes)** field, enter the idle threshold value. The valid range is from 0 to 4,294,967,295 bytes. The default value is 0.
n) In the **Reassociation Timeout time [1-100 seconds]** field, enter the reassociation timeout time. The valid range is from 1 to 100 seconds. The default value is 20 seconds.
o) From the **mDNS Mode** drop-down list, choose an mDNS mode: **Bridging**, **Drop**, or **Gateway**



Note These parameters aren't supported on the Cisco AireOS Wireless Controller.

Step 16 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Advanced SSID Configuration - Feature Templates** area.

Step 17 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for Cisco CleanAir

CleanAir is a spectrum intelligence solution designed to manage the challenges of a shared wireless spectrum proactively. It allows you to see all the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act on this information. For example, you can manually remove the interfering device, or the system can automatically steer the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

Default CleanAir 802.11a Design, **Default CleanAir 802.11b Design**, and **Default CleanAir 6GHz Design** are the default CleanAir configuration feature templates. You can't edit or delete the default designs. However, you can create a custom feature template for your specific network design.

Before you begin

You should have discovered the devices in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **CleanAir Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add CleanAir Configuration** window, enter a name for the design.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.

Step 7 Click the **CleanAir Enable** toggle button to enable the CleanAir functionality on the 2.4-GHz or 5-GHz radio band.

If the **CleanAir Enable** toggle button is enabled, click it to disable the feature and prevent the wireless controller from detecting spectrum interference.

Step 8 Click the **CleanAir Device Reporting Enable** toggle button to enable the CleanAir system to report detected sources of interference, if any.

If the **CleanAir Device Reporting Enable** toggle button is enabled, click it to disable the feature and prevent the wireless controller from reporting interferers.

Step 9 Click the **Persistent Device Propagation** toggle button to enable propagation of information about persistent devices that can be detected by CleanAir.

Persistent device propagation enables you to propagate information about persistent devices to the neighboring APs that are connected to the same wireless controller. Persistent interferers are present at the location, and interfere with WLAN operations even if they aren't detectable at all times.

Step 10 Expand **Enable Interferers Features** and check the check box next to the source of interference that needs to be detected and reported by the CleanAir system:

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- Microwave Oven
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- Video
- Wimax Fixed
- Wimax Mobile
- Xbox

Step 11 In the **CleanAir Description** field, enter a description.

Step 12 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **CleanAir Configuration - Feature Templates** area.

Step 13 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for Dot11ax configuration

The **Dot11ax Configuration** feature template configures 802.11ax parameters on devices. **Default Dot11ax 6-GHz Design**, **Default Dot11ax 802.11a Design**, and **Default Dot11ax 802.11b Design** are the default 802.11ax configuration feature templates. You can't edit or delete the default designs. However, you can create a custom feature template for your specific network design.

The Dot11ax configuration involves the 802.11ax wireless specifications standard, also known as High Efficiency (HE) Wireless. Dot11ax is a dual-band technology that uses 2.4-GHz, 5-GHz, and 6-GHz bands. You can configure Dot11ax configuration parameters only on Wi-Fi 6-supported Cisco Catalyst 9100 Series Access Points.

Note BSS color is used to identify an overlapping basic service set (OBSS). BSS configurations are pushed on Wi-Fi 6-supported APs only. The Cisco Catalyst 9100 Series Access Points are the next-generation Wi-Fi 802.11ax APs, and ideal for high-density, high-definition applications.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Dot11ax Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Dot11ax Configuration** window, enter a name for the feature template.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 Click the **BSS Color** toggle button to enable the BSS color functionality. The default value is disabled.

BSS color functionality is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later.
- Cisco Wireless Controllers that run Cisco IOS XE Release 17.1 and later.

Step 7 Click the **Target Wakeup Time** toggle button to enable the target wake-up time. The default value is disabled.

Target wake-up time is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later.
- Wireless controllers that run Cisco IOS XE Release 17.1 and later.

Step 8 Click the **Target Wakeup Time Broadcast** toggle button to enable the target wake-up time broadcast. The default value is disabled.

Target wake-up time broadcast is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later.
- Wireless controllers that run Cisco IOS XE Release 17.3.1 and later.



Note For wireless controllers that run a version between Cisco IOS XE Release 17.3.1 and Cisco IOS XE Release 17.6, the YANG default value of the target wake-up time broadcast is enabled. When you upgrade Catalyst Center with these wireless controllers from a release earlier than Release 2.3.5, the default value is set to disabled even if the YANG default value is enabled. This difference is listed as a compliance mismatch between the actual and intended values of the attribute.

To configure the intended value on the wireless controllers, reprovision the wireless controllers after the upgrade.

Step 9 Click the **Multiple BSSID** toggle button to enable the multiple basic service set identifier (BSSID) functionality. The default value is disabled.

Multiple BSSID is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.



Note This toggle button is available only when you choose the **6 GHz** radio band.

Step 10 From the **Radio Band** drop-down list, choose **2.4 GHz**, **5 GHz**, or **6 GHz**. The default value is disabled.

Step 11 Click the **OBSS PD** toggle button to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.

OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.4 and later.

Note This toggle button isn't available for the **6 GHz** radio band.

Step 12 In the **Non-SRG OBSS PD Max Threshold (dbm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm. The default value is -62 dBm.

Non-SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.4 and later.

Note This toggle button isn't available for the **6 GHz** radio band.

Step 13 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Dot11ax Configuration – Feature Templates** area.

Step 14 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the APs. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for Dot 11be status configuration

The **Dot11be Status Configuration** feature template configures the 802.11be status for the 2.4-GHz, 5-GHz, and 6-GHz radio bands. The 802.11be configuration is applicable for the devices that are running Cisco IOS XE Release 17.15.2.

Default 802.11be Status 2.4GHz Design, **Default 802.11be Status 5GHz Design**, and **Default 802.11be Status 6GHz Design** are the default 802.11be status configuration feature templates. You can't edit and delete the default designs. However, you can create a custom feature template for your specific network design.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and choose **Dot11be Status Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add 802.11be Status Configuration** slide-in pane, enter a name for the feature template.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 To enable or disable the 802.11be status, use the **Dot11be Status** toggle button.



Important Configuring the 802.11be status disables the WLAN momentarily and causes loss of connectivity for the clients on the corresponding radio band.

Step 7 From the **Radio Band** drop-down list, choose the radio band for which you want to configure the 802.11be status: **2.4 GHz**, **5 GHz**, or **6 GHz**

Step 8 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Dot11be Status Configuration - Feature Templates** area.

Step 9 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Inventory**. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Create a feature template for event-driven RRM configuration

The **Event Driven RRM Configuration** feature template configures event-driven RRM parameters for the 2.4-GHz and 5-GHz radios. **Default Event Driven 2.4GHz Design** and **Default Event Driven 5GHz Design** are the default event-driven RRM configuration feature templates. You can't edit or delete the default designs. However, you can create a custom feature template for your specific network design.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Event Driven RRM Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Event Driven RRM Configuration** slide-in pane, enter a name for the feature template.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 From the **Radio Band** drop-down list, select the radio band: **2.4GHz** or **5GHz**

Step 7 Click the **Event Driven RRM** toggle button to run RRM when a CleanAir-enabled AP detects a significant level of interference.

Step 8 From the **Sensitivity Threshold** drop-down list, choose the sensitivity threshold level at which you want the RRM to be triggered from these options.

When the interference for the AP rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected AP radio, if possible, to improve network performance.

- **Low**: Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.
- **Medium**: Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.
- **High**: Specifies the most sensitivity to non-Wi-Fi interference as indicated by the AQ value.
- **Custom**: Specifies custom sensitivity to non-Wi-Fi interference as indicated by the AQ value. If you choose this option, you must specify a custom value in the **Custom Threshold [1-99]** field.

Step 9 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Event Driven RRM Configuration - Feature Templates** area.

Step 10 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for Flex configuration

Use the **Flex Configuration** feature template to configure the FlexConnect configuration on Cisco IOS XE-based wireless controllers.

The **Default Flex Configuration** is the default FlexConnect configuration feature template. You can't edit or delete the default designs. However, you can create a custom feature template for your specific network design.

Before you begin

Using the **Discovery** feature, discover the devices in your network so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Flex Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Flex Configuration** slide-in pane, enter a name for the design.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 Click the **IP Overlap** toggle button to configure IP overlap.

Step 7 Click **Apply**.
The created design instance is displayed in the **Design Instances** window under the **Flex Configuration - Feature Templates** area.

Step 8 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.

   To use the feature template as global configuration for the device, add it to the network profile of the device site. To use the feature template for an SSID-specific configuration, add it to the network profile of the managed AP locations or sites.

2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for Global IPv6 Configuration

Use the **Global IPV6 Configuration** feature template to enable IPv6 globally on devices.

The **Default Global IPv6 Design** is the default Global IPV6 configuration feature template. You can't edit and delete the default designs. However, you can create a custom feature template for your specific network design.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Global IPV6 Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

The window appears.

Step 4 In the **Design Name** field of the **Add Global IPV6 Configuration** slide-in pane, enter a name for the feature template.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 Click the **Global IPV6 Config** toggle button to enable IPv6 globally on devices.

Step 7 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Global IPV6 Configuration - Feature Templates** area.

Step 8 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can deploy on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for Multicast

Use the **Multicast Configuration** feature template to configure multicast parameters on devices.

If your network supports packet multicasting, you can configure the multicast method that the Cisco Wireless Controller uses. The wireless controller runs multicasting in one of these modes:

- Unicast mode: In this mode, the wireless controller unicasts every multicast packet to every access point associated to the wireless controller. This mode is not very efficient, but is required on networks that do not support multicasting.
- Multicast mode: In this mode, the wireless controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the wireless controller processor and shifts the work of packet replication to your network. This method is more efficient than the unicast method.

The **Default Multicast Design** is the default Multicast configuration feature template. You can't edit and delete the default designs. However, you can create a custom feature template for your specific network design.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Multicast Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add Design**.

Step 4 In the **Design Name** field of the **Add Multicast Configuration**, enter a name for the design.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 Click the **Enable Global Multicast Mode** toggle button to configure sending multicast packets. The default value is disabled.

Step 7 From the **AP Multicast Mode** drop-down list, choose **UNICAST** or **MULTICAST**.

- Choose **UNICAST** to configure the wireless controller to use the unicast method to broadcast packets.
- Choose **MULTICAST** to configure the wireless controller to use the multicast method to broadcast packets to a CAPWAP multicast group.

Step 8 Expand **IPV4 Multicast Group Address** and enter the IPv4 multicast address in the **IP Address** field.

Step 9 Expand **IPV6 Multicast Group Address** and enter the IPv6 multicast address in the **IP Address** field.

Step 10 Click **Apply**.

The created design instance is displayed in the **Design Instances** window under the **Multicast Configuration - Feature Templates** area.

Step 11 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for RRM FRA parameters

The **RRM FRA Configuration** feature template configures the Flexible Radio Assignment (FRA) parameters for Radio Resource Management (RRM) for 2.4-5 GHz and 5-6 GHz radio bands.

The **Default FRA 2.4-5GHz Design** and **Default FRA 5-6GHz Design** are the default FRA feature templates. You can't edit and delete the default designs. However, you can create a custom feature template for your specific network design.



Note

- The 6-GHz radio band is not supported in Cisco AireOS Wireless Controllers.
- The Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.6 and later support the 6-GHz radio band.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **RRM FRA Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add Flexible Radio Assignment (FRA) Configuration** slide-in pane, enter a name for the design.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 From the **Radio Band** drop-down list, choose a radio band.

Step 7 Click the **FRA Freeze** toggle button to enable the FRA freeze functionality. This functionality is disabled by default.

Cisco Wireless Controllers that run Cisco IOS XE Release 17.6.1 and later support this functionality.

Note This toggle button is available only for the **2.4-5 GHz** radio band.

Step 8 Click the **FRA Status** toggle button to enable the FRA status functionality. This functionality is enabled by default.

Step 9 From the **FRA Interval** drop-down list, choose an FRA interval.

Step 10 From the **FRA Sensitivity** drop-down list, choose an FRA sensitivity value.

This parameter sets the FRA coverage overlap sensitivity.

Note This drop-down list is available only for the **2.4-5 GHz** radio band.

Step 11 Click **Save**.

The created design instance displays in the **Design Instances** window in the **RRM FRA Configuration – Feature Templates** area.

Step 12 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the access points. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Create a feature template for RRM general parameters

The **RRM General Configuration** feature template configures the Radio Resource Management (RRM) general parameters for the 2.4-GHz, 5-GHz, and 6-GHz radios.

The **Default RRM General 2.4 GHz Design**, **Default RRM General 5 GHz Design**, and **Default RRM General 6 GHz Design** are the default RRM general configuration feature templates. You can't edit and delete the default designs. However, you can create a custom feature template for your specific network design.

Note

- The 6-GHz radio band is not supported on Cisco AireOS Wireless Controllers.
- Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Release 17.6 and later releases support the 6-GHz radio band.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **RRM General Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 In the **Design Instances** window, click **Add**.

Step 4 In the **Design Name** field of the **Add RRM General Configuration** slide-in pane, enter a name for the design.

Step 5 To lock all the properties in the feature template, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.

A property that is locked in the design can't be changed during device provisioning.

Step 6 In the **Radio Band** tab, choose the radio band from the **Radio Band** drop-down list: **2.4 GHz**, **5 GHz**, or **6 GHz**.

Step 7 In the **Threshold** tab, set the throughput threshold value for the radio band selected in the Throughput Threshold (1000-10000000 Bps) field.

Step 8 In the **Monitoring** tab, configure the monitoring channels and neighbor discover type.

- From the **Monitoring Channels** drop-down list, choose one of these options to specify the set of channels that the AP uses for RRM scanning. By default, the monitoring channel is set to Country.
  - **All**: RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
  - **Country**: RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
  - **DCA**: RRM channel scanning occurs only on the channel set used by the DCA algorithm.
- From the **Neighbor Discover Type** drop-down list, choose the neighbor discovery type. By default, the mode is set to Transparent.
  - **Transparent**: Sets the neighbor discover type to transparent. Packets are sent as is.
  - **Protected**: Sets the neighbor discover type to protected. Packets are encrypted.

Step 9 In the **Coverage** tab, click the **Global Coverage Hole Detection Enabled** toggle button to enable coverage hole detection. By default, this value is selected.

If you enable coverage hole detection, the Cisco Wireless Controller automatically determines, based on data received from the APs, if any APs have clients that are potentially located in areas with poor coverage.

Step 10 Click **Save**.

The created design instance displays in the **Design Instances** window under the **RRM General Configuration - Feature Templates** area.

Step 11 (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

What to do next

1. Attach the created feature template to a network profile so that it can be deployed on the wireless controller. From the main menu, choose **Design** > **Network Profiles**. For more information, see Create network profiles for wireless, on page 460.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 620.

Create a feature template for rogue general parameters

Use this procedure to configure rogue general configuration and client exclusions policies.

The default feature templates for rogue general configuration, include:

- **Default Rogue General Configuration Critical**
- **Default Rogue General Configuration Custom**
- **Default Rogue General Configuration High**
- **Default Rogue General Configuration Low**

You can’t edit and delete the default designs. However, you can create a custom feature template for your specific network design.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Feature Templates**.

Step 2 In the left pane, expand **Wireless** and select. **Rogue General Configuration**.

Alternatively, you can search for a feature template by entering its name in the **Search** field.

Step 3 Click **Add** to create new rogue general configuration profile.

The **Add Rogue General Configuration** slide-in pane displays.

Step 4 In the **Add Rogue General Configuration** slide-in pane, do these steps:

a) In the **Design Name** field, enter a name for the design.
b) In the **General** tab, choose the **Rogue Detection Security Level** from the drop-down list.
c) In the Expiration timeout for Rogue APs field, enter the time in seconds for the chosen rogue detection security level as follows:

- **LOW**: If you choose low security level, expiration timeout must be 240 seconds.
- **HIGH**: If you choose high security level, expiration timeout must be 1200 seconds.
- **CRITICAL**: If you choose critical security level, expiration timeout must be 3600 seconds.
- **CUSTOM**: If you choose custom security level, expiration timeout must be between 240 to 3500 seconds.

d) Toggle the **Validate Rogue Clients against AAA** toggle button to validate the rogue clients.
e) Toggle the **Detect and Report Adhoc Networks** toggle button to report an adhoc network.
f) Toggle the **Validate Rogue APs against AAA** toggle button to validate the rogue APs.

Note **Validate Rogue APs against AAA** toggle button and **Rogue Polling Interval (seconds)** field is only displayed if you select security level as custom.

g) In the **Rogue Polling Interval (seconds)** field, enter a valid rogue polling time interval in seconds.

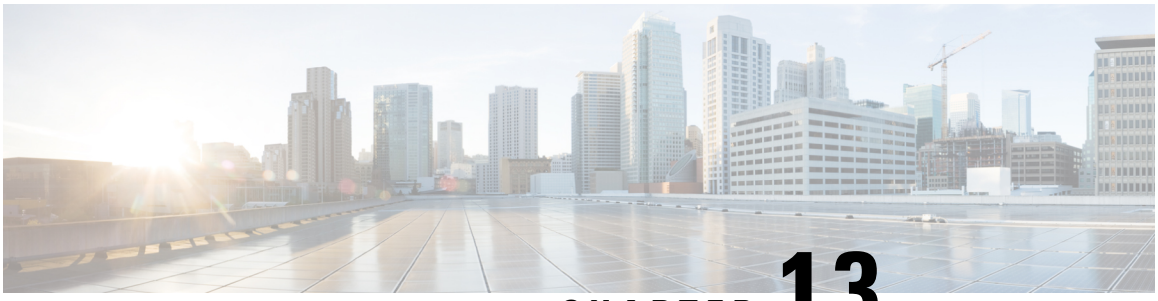
The valid rogue polling interval value ranges from 60 to 86400 seconds.

h) In the **Rogue Detection Client Number Threshold** field, enter the valid threshold value between 0 to 256.
i) In the **Rogue Init Timer (seconds)** field, enter the time in seconds. The default value is 180 seconds.
j) In the **AP Authentication Alarm Threshold** field, enter a valid threshold value between 1 to 255.
k) Toggle the **Syslog Notification** toggle button to get notification, if any system logs are generated.
l) In the **MFP Key Refresh Interval (hours)** field, enter a valid time interval in hours, between 1 to 24.
m) (Optional) To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.
n) Click **Save**.

What to do next

1. (Optional) To add feature template to a network profile, see Add feature templates to a network profile, on page 464.
2. Provision the feature template specified in the network profile to network devices. From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

   For more information, see Provision a Cisco AireOS Controller, on page 620.



CHAPTER 13

Manage Software Images

- About Software Image Management, on page 533
- Integrity Verification of software images, on page 534
- View software images, on page 534
- Use a recommended software image, on page 538
- Import a software image, on page 539
- Manage software image assignment for a device family, on page 540
- Schedule Image Update, on page 542
- Upload software images for devices in Install Mode, on page 544
- About standard software images, on page 545
- Mark a software image as standard, on page 545
- Manage the standard software image, on page 547
- Configure an image distribution server, on page 548
- Add image distribution servers to sites, on page 550
- Provision a software image, on page 551

About Software Image Management

Catalyst Center stores all the software images, software maintenance updates (SMUs), subpackages, ROMMON images, and so on, for the devices in your network. Software Image Management provides these functions:

- Software Image Management: Catalyst Center stores all the unique software images according to image type and version. You can view, import, and delete software images.
- Provision: You can push software images to the devices in your network.

Before using Software Image Management features, you must enable Transport Layer Security protocol (TLS) on older devices such as Cisco Catalyst 3000, 4000, and 6000. After any system upgrades, you must re-enable TLS. For more information, see “Configure Security for Catalyst Center” in the Cisco Catalyst Center Administrator Guide.

Note In Release 2.3.3 and later, Catalyst Center supports only internal bootflash as the primary boot option for Software Image Management (SWIM) and Software Maintenance Updates (SMUs) on the IE3x00 series, and IE9x00 series switches.

If you have an earlier release of Catalyst Center (before Release 2.3.3), and if an IE3x00, or IE9x00 device in your network is already booted with a Secure Digital (SD) flash memory module, then ensure that you set the internal bootflash as the primary boot option on the device, using the **boot flash-primary** command.

To save and synchronize a running configuration from SD flash to bootflash, use the **sync** command.

Integrity Verification of software images

The Integrity Verification application monitors software images that are stored in Catalyst Center for unexpected changes or invalid values that could indicate your devices are compromised. During the import process, the system determines image integrity by comparing the software and hardware platform checksum value of the image that you are importing to the checksum value identified for the platform in the Known Good Values (KGV) file to ensure that the two values match.

On the **Software Image Management** page, a message displays if the Integrity Verification application cannot verify the selected software image using the current KGV file. For more information about the Integrity Verification application and importing KGV files, see the *Cisco Catalyst Center Administrator Guide*.

View software images

After you run Discovery or manually add devices, Catalyst Center automatically stores information about the software images, SMUs, and subpackages for the devices.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 The **Overview** tab consists of these sections:

- The top section displays these details:
  - **Images**: Shows the number of images for device families along with critical and high advisories.
  - **Devices**: Shows the number of tagged images, images ready for update, failed update readiness, and failed image updates.
  - **Updates**: Shows the number of image updates that failed, in-progress, and are successful.
- The **Image Update Tools** section at the bottom enables you to execute these tasks:
  - **Schedule Image Update**: Schedule the update of a software image at a specific date and time on selected devices. For more information, see Schedule Image Update, on page 542.

- **Check Image Update Status**: Click **Check Update Status** to trigger the precheck conditions and to resynchronize the image with the device. The **Devices Updates** slide-in pane shows the updates that are in-progress, waiting, terminated, successful, and failed.

  A table shows the details of device name, IP address, updated date, duration for the update, software image version, task name, status of the update, and actions. Click a device name to view more details. In the **Actions** column, you can click the **Retry** option for a device to re-run the update.

  Click **Upcoming Tasks** to view the scheduled updates.

- **Download Update Readiness Report**: Click **Download Readiness Report** to download the device readiness results for all devices to a CSV file.

- **Import an Image**: Click **Import Image** to import a software image or software image update. For more information, see Import a software image, on page 539.

- The **Yet to be submitted Image Update flows** section shows the upcoming tasks that are yet to be submitted. You can click the ellipsis icon in this section and decide to resume or delete the task.

Step 3 The **Images** tab consists of these options.

a) The **Images** section displays the number of total device families, images running, device families without standard, critical and high advisories.

   Click **Show images summary** or **Hide images summary** at the right to view or hide the summary.

b) The bottom section displays the details of the product family name for the images, along with number of devices, images, images marked standard, and critical and high advisories for each device family.

   You can perform these tasks:

   - **Show imported images**: Click to view the details about imported software images.

     In the **Imported Image Family** window, the **Images** table shows **Image Name**, **Version**, **Device Series Assigned**, and **Action** for all the imported software images.

     In the **Action** column, click **Assign** to assign a software image to a device family. For more information, see Manage software image assignment for a device family, on page 540.

   - **Show task**: Click to view status of all the tasks that are related to software images.

     The **Recent Tasks** slide-in pane shows status of the last 50 tasks. From the **Task Status** drop-down list, select **All**, **Failed**, **In-Progress**, or **Successful** to filter the tasks based on status.

   - **Import images**: Click to import a software image or software image update. For more information, see Import a software image, on page 539.

From the **Product Family Name** column, click a device name to view more details.

- A new window opens with all the available image for the selected device, displaying the image name and version.
- The **Attributes** column shows the image details. You can download the image from Cisco.com for the image with the attribute as **Recommended**.
- From the **Actions** column, you can select to mark the images as standard and download them. For more information, see Mark a software image as standard, on page 545.
  - **Image details not available**: Click to download a matching image.

- **Available for download**: The image is available on Cisco.com for download. You can mark the image as standard and download it from Cisco.com.
- **Downloaded**: The latest image is already downloaded. Click to mark the image as standard or standard with conditions.
- **Marked as standard**: The image is marked as a standard one. Click the drop-down arrow to remove the standard tag or to edit the standard conditions.

Click the **Sync Updates** option at the top to view the latest status of the images.

Step 4 The **Devices** tab consists of these options.

a) The **Devices** section displays the number of total eligible devices and the number of devices with different image status. The image status are: image not tagged as standard, images ready for update, update readiness failed, failed images, image updates in progress, and devices running with standard image.

Click **Show devices summary** or **Hide devices summary** at the right to view or hide the summary.

b) The bottom section shows the details of the device name, tags, device family, software version, image status, image name, reachability, readiness check status, management address, latest update status, and image compatibility.

c) Click **Tag** to create a new tag for a device or manage the existing tags. For more information, see Tag devices, on page 158.

d) Select one or more devices and click **Check Image Update Readiness** to trigger the precheck conditions and to resynchronize the image with the device. This option enables to display the latest resynchronized time, when you click the **Ready** option in the **Devices** tab. The **Devices Updates** slide-in pane shows the updates that are in-progress, waiting, terminated, successful, and failed.

e) Click **Download Update Readiness Report** to download the device readiness results for all devices to a CSV file.

f) Select the devices and click **Update Devices** to start the image upgrade process. This option redirects you to the **Image Update** window. This image upgrade procedure also allows you to schedule the image update at a specific date and time. For more information, see Schedule Image Update, on page 542.

Click a device name to view more details of the device.

From the **Device Family** column, click a device name to view more details.

- A new window opens with all the available image for the selected device, displaying the image name and version.
- The **Attributes** column shows the image details. You can download the image from Cisco.com for the image with the attribute as **Recommended**.
- From the **Actions** column, you can select to mark the images as standard and download them. For more information, see Mark a software image as standard, on page 545.

Click the **Sync Updates** option at the top to view the latest status of the images.

Step 5 The **Updates** tab shows the details of recent image updates that failed, are successful, are in-progress, and are scheduled. You can click the link to a task to view more information.

Step 6 If you have already configured the Cisco.com user, skip ahead to Step 3. If you haven't, complete these steps:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).

b) Open another Catalyst Center GUI instance and log in.

c) Open another instance of the **Software Image Management** page.

d) Complete one of these tasks:

If you...	Then...
completed a fresh installation of Catalyst Center,	configure a new Cisco.com user by clicking the **Add** link in the **Cisco.com ID** field.
upgraded to the latest version of Catalyst Center and want to use the same Cisco.com user that was configured previously,	reauthenticate that user by clicking the **Re-Authenticate** link in the **Cisco.com ID** field.
upgraded to the latest version of Catalyst Center and don't want to use the same Cisco.com user as before,	delete the old Cisco.com user and then configure a new one. 1. Click the **Delete** link in the **Cisco.com ID** field. 2. Confirm the operation by clicking **Delete** in the resulting dialog box. 3. Click the **Add** link in the **Cisco.com ID** field.

e) In the **Information** pop-up window, check one or both of these check boxes and then click **Authenticate**:

- (Mandatory) **I am in private or incognito mode**
- (Optional) **Save credentials**

f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

The **Device activated** pop-up window appears.

i) Close the **Device Activated** pop-up window.
j) Refresh the **Software Image Management** page.
k) In the **Cisco.com ID** field, confirm that the email address you entered for the user displays. Also confirm that you see the **Change** link.

Step 7 Click **Routers**, **Switches**, **Wireless Controllers**, **Security and VPN**, **Sensors**, or **Virtual Devices** in the top of the window or click the search or filter icon in the **Images** tab to filter device families.

By default, the **Images** tab shows all the device families.

Note Third-party (non-Cisco) devices are not shown in the **Images** window, because image activation and image update features are not supported for third-party devices.

Step 8 Click **Sync Updates** and then click **OK** in the subsequent warning message to synchronize image information from cisco.com for all managed devices in Catalyst Center.

If cisco.com credentials are not set, you are prompted to specify them.

You can view the progress of task in **Show Tasks**. After the task success, the image information updates for all device families.

Note You can fetch image information only once in an hour.

Use a recommended software image

Catalyst Center displays and allows you to choose Cisco-recommended software images for the devices that it manages.

Note Only the latest Cisco-recommended software images are available for download.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco.com Credentials**.

Step 2 Verify that you have entered the correct credentials to connect to cisco.com.

Step 3 From the main menu, choose **Provision** > **Software Image Management**.

Step 4 Click **Images**.

Catalyst Center displays each product family with its corresponding number of devices, images, images marked as standard, and so on.

Step 5 Under **Product Family Name**, click the product family to view all its available images.

This table lists some device types and their unsupported software images.

Device type	Limitations
APs managed by Catalyst Center	SWIM upgrade or downgrade is not supported.
Cisco Meraki devices	SWIM upgrade or downgrade is not supported.
Third-party devices	SWIM upgrade or downgrade is not supported.
Cisco Catalyst 9400 Series switches	Bootloader image upgrade or downgrade is not supported.
Cisco Catalyst 9800 Series switches	ROMMON image upgrade is supported. However, image downgrade is not supported.
Cisco ASR Series routers	Complex Programmable Logic Device (CPLD) image upgrade is not supported.
Cisco ISR Series routers	CPLD image upgrade is not supported.

Step 6 Mark the recommended image as standard.

For more information, see Mark a software image as standard, on page 545.

Step 7 Provision the recommended software image on devices in your network.

For more information, see Provision a software image, on page 551.

Import a software image

If Catalyst Center is deployed in an air-gapped environment or has no access to the cloud, you can import software images and software image updates from either your local computer or a URL. Otherwise, we recommend that you download software images from cisco.com.

Imported images are categorized based on different supervisors that are present in a specific device family. Categorization under different supervisors supports only the Cisco Catalyst 9400 series family.

If you use FTP to import an image from an FTP server, use the FTP standard:

```
ftp://username:password@ip_or_hostname/path
```

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click the **Images** tab and then click **Import images**.

Alternately, click the **Overview** tab and click **Import Image** in the **Image Update Tools** section.

Step 3 On the **Import Image** slide-in pane, import the software image by completing these steps.

a. Under **Upload Option**, indicate how you want to upload the image.

This table describes the upload options.

Option	Description
Select from computer	Upload a local software image or software image update file.
Enter URL	Import software image or software image updates from an HTTP or FTP source. **Note** Software images are compliant with the Federal Information Processing Standard (FIPS). If FIPS mode is enabled in Catalyst Center, you cannot import images from a URL. Import images from your computer or cisco.com.
Select ISSU compatibility matrix	Upload a local compatibility matrix file. The In-Service Software Upgrade (ISSU) compatibility matrix provides information about the compatibility between the current and target software versions, ensuring that the upgrade can proceed without issues.

b. Upload the file based on the chosen option.

If you chose...	Then...
Select from computer or **Select ISSU compatibility matrix**,	you can either: • drag and drop the file, or • click **Choose a file** and choose the locally-stored file.
Enter URL,	in the **Enter Image URL (http or ftp)** field, enter the image URL.

c. Under **Source**, indicate the source of the image.

If the image that you are importing is for a third-party vendor, click **Third party**. Then choose an **Application Type**, describe the device **Family**, and identify the **Vendor**.

Note Image activation and image update features are not supported for third-party devices.

d. Click **Import**.

Step 4 Click **Show Tasks** to verify that the image was imported successfully.

If you imported an SMU, Catalyst Center automatically applies the SMU to the correct software image. To view the SMU, return to the **All available images** table and expand the image row with the SMU.

Note Catalyst Center does not allow you to import software images for the FTD devices that are managed by FMC. When you add FMC to inventory and it goes to the Managed state, go to the **Software Image Management** page, click **Images**, and click the relevant hyperlinked product family name in the table to view the software images available for the FMC.

Manage software image assignment for a device family

After importing a software image from either your local computer or a URL (excluding cisco.com), you can assign or reassign it to an available device family. The imported image can be assigned to multiple devices at any time.

Before you begin

You have imported a software image from either your local computer or a URL (excluding cisco.com). For more information, see Import a software image, on page 539.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click **Images**.

Step 3 Click **Show imported images**.

Step 4 Manage the imported image using this table for instructions.

If you want to...	Then...
assign an imported image,	**a.** Click **Assign** in the corresponding image name row. **b.** In the **Assign Device Family** slide-in pane, click **Cisco Devices Series** or **All Device Series**. Under **All Device Series**, you can filter the table by device type using the **Select a device type** drop-down list. **Note** **Cisco Devices Series** displays device series information only if there is internet connection. **c.** Check the check boxes for the device series to which you want to assign the software image. You can check the **Device Series** check box to choose all device series in the table. **d.** If the device series is not assigned to a site, click **Select Site**, and then in the **Select Site** dialog box, choose the appropriate site and click **Select**. **e.** Click **Assign**. **Note** • **Assign** is disabled if the device series is not assigned to a site. • If cisco.com credentials are not set, specify the credentials in **System** > **Settings** > **Cisco.com Credentials**.

If you want to...	Then...
reassign an imported image,	**a.** Click **Edit** in the corresponding image name row. **b.** In the **Assign Device Family** slide-in pane, click **Cisco Devices Series** or **All Device Series**. **c.** Check the check boxes for the device series to which you want to reassign the software image. **d.** Click **Select Site**. **e.** In the **Select Site** dialog box, update the site assignment for this device family and then click **Select**. **f.** Click **Assign**.

Schedule Image Update

Use this procedure to schedule the update of a software image at a specific date and time on selected devices.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click the **Images** tab. Select the image to be upgraded and mark the image as standard. To mark the image, see Mark a software image as standard, on page 545.

Step 3 In the **Devices** tab, select the devices that need to be updated with the image and click **Update Devices**.

Alternately, you can go to the **Overview** tab and click **Schedule Update** in the **Image Update Tools** section. You are redirected to the Image upgrade workflow.

Step 4 The **Image Update** window opens which prompts you with instructions to schedule the image update.

Step 5 In the **Task Name** window, enter a unique name for the scheduled update task and click **Next**.

Step 6 In the **Select Devices** window, select the location of the devices from the left panel. In the **Devices** section, check the checkboxes for the devices you want to schedule the image update and click **Next**.

Note If the prechecks succeed for a device, the **Outdated** link in the **Software Image** column has a green check mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link has a red check mark, and you cannot update the software image for that device. Click the **Outdated** link and correct the errors before proceeding. See List of Device Upgrade Readiness Prechecks.

Step 7 In the **Software Distribution Checks** window, you can enable pre-checks and post-checks for the software distribution and select the check order. After choosing the distribution checks, click **Next**.

Note If you associated the external image distribution server with a network hierarchy, the image distribution server distributes the image to all devices under the network hierarchy. See Add image distribution servers to sites, on page 550.

To select the validators that you want to run for the current workflow or add new custom checks, do these steps:

a) Hover your mouse over the information icon to view the validation criteria and the CLI commands that are used for the validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do these steps:

1. Click **add a custom check** to launch the **New Custom Check** window.
2. Enter the **Name** for the custom check.
3. From the **When** drop-down list, select **pre**, **post**, or both.
4. From the **Select a Test Device** drop-down list, select the device you want to check.
5. Click **Open Command Runner**, and enter the CLI commands.
6. Expand **Add Known Command-Patterns to Ignore During Checks** to add a command pattern that is used to ignore the matching output for the checks.

   To add a command pattern:

   - To create a new pattern, enter a desired name and string or pattern.
   - To use an existing pattern, click **most commonly used patterns**, select the desired pattern, and click **Add Selected**.
   - Click **Test All Patterns**.

7. Expand the **Additional Criteria** area.

   From the **Operation** drop-down list, select **Distribution**, **Activation**, or both.

8. From the **Device Series** drop-down list, select the desired device series and click **Save**.

Step 8 In the **Software Activation Checks** window, you can enable pre-checks and post-checks for the software activation and select the check order. After choosing the activation checks, click **Next**.

Step 9 In the **Device Activation Order** window, you can use filters to sort devices and arrange the order of their activation in parallel or sequentially. After sorting the devices, you can reorder them sequentially. Click **Next**.

Step 10 In the **Schedule Task and Clean Up** window, schedule these tasks:

- In the **Software Distribution** section, enable the checks for the software distribution.
- In the **Software Activation** section, select either **Now** or **Later** to schedule the update. If you select **Later**, configure the start date and time, and select the time zone for the update to start. By default, the time zone is set as the time zone of the selected site.
- Check the **Initiate Flash Cleanup After Activation** checkbox to store only the running image and remove all previous images saved on the device.

After configuring the settings, click **Next**.

Step 11 The **Summary** window shows the summarized data of the scheduled update. Review the details and if required, you can click **Edit** to modify the settings. Click **Submit**.

Upload software images for devices in Install Mode

The **Software Image Management** page might show a software image as being in Install Mode. When a device is in Install Mode, Catalyst Center cannot upload its software image directly from the device. When a device is in Install Mode, you must first manually upload the software image to the Catalyst Center repository before marking the image as standard.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click **Images**.

Step 3 Under **Product Family Name**, click the hyperlinked product family name to view its available images.

Step 4 Under **Image Name**, find the software image of the device that is running in **Install Mode**.

Step 5 From the **Image details not available** drop-down list, choose **Import matching image**.

Step 6 On the **Import Image** slide-in pane, import the image by completing these steps.

a. Under **Upload Option**, indicate how you want to upload the image.

This table describes the upload options.

Option	Description
Select from computer	Upload a local software image or software image update file.
Enter URL	Import software image or software image updates from an HTTP or FTP source. **Note** Software images are compliant with Federal Information Processing Standard (FIPS). If FIPS mode is enabled in Catalyst Center, you cannot import images from a URL. Import images from your computer or cisco.com.
Select ISSU compatibility matrix	Upload a local compatibility matrix file.

b. Upload the file based on the chosen option.

If you chose...	Then...
Select from computer or **Select ISSU compatibility matrix**,	you can either: • drag and drop the file, or • click **Choose a file** and choose the locally-stored file.

If you chose...	Then...
Enter URL,	in the **Enter Image URL (http or ftp)** field, enter the image URL.

c. Under **Source**, indicate the source of the image.

If the image that you are importing is for a third-party vendor, click **Third party**. Then choose an **Application Type**, describe the device **Family**, and identify the **Vendor**.

Note Image activation and image update features are not supported for third-party devices.

d. Click **Import**.

Step 7 Click **Show task** and verify that the software image you imported is green, indicating it has been successfully imported and added to the Catalyst Center repository.

Step 8 Click **Refresh**.

The page for the device family and its available images is refreshed. Catalyst Center displays the software image.

About standard software images

Catalyst Center allows you to designate software images and SMUs as *standard*. A standard software image or SMU is a validated image that meets the compliance requirements for the particular device type. Designating a software image or SMU as standard saves you time by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can designate an image and a corresponding SMU as standard to create a standardized image. You can also specify a standard image for a specific device role. For example, if you have an image for the Cisco 4431 Integrated Service Routers device family, you can further specify a standard image for those Cisco 4431 devices that have the Access role only.

You cannot mark a SMU as standard unless the image to which it corresponds is also marked standard.

Mark a software image as standard

You can mark a software image for a device family or device role as standard. The device role identifies and groups devices according to their responsibilities and placement within the network.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click **Devices**.

Alternatively, you can click **Images**.

Step 3 Under **Device Family**, click the hyperlinked device family for which you want to mark a software image as standard.

Alternatively, if chose **Images**, click the hyperlinked product family under **Product Family Name** for which you want to mark a software image as standard.

Step 4 Mark the software image as standard with or without conditions.

Use this table to download and mark the image as standard based on if the image is uploaded to the Catalyst Center repository.

If the software image is...	And you want to...	Then...
uploaded into the Catalyst Center repository,	mark the image as standard with or without conditions,	**a.** Under **Image Name**, locate the image that you want to mark as standard. **b.** From the corresponding **Downloaded** drop-down list for the image, choose **Mark as standard** or **Mark as standard with conditions**. **c.** In the **Mark as standard** slide-in pane, if required, configure the advanced settings to assign the image to a device role, device tags, or both. Then, click **Confirm**. • **Device role**: From the drop-down list, choose a role. • **Device tags**: From the drop-down list, check the device tag check boxes.
not uploaded into the Catalyst Center repository,	download the image and mark it as standard,	**a.** Under **Image Name**, locate the image that you want to download and mark as standard. **b.** From the corresponding **Available for download** drop-down list for the image, choose **Mark as standard**. **c.** In the **Mark as standard** slide-in pane, click **Confirm**. The system automatically downloads the image and then marks it as standard. Under **Actions**, the software image download in-progress bar is displayed. This process might take some time. **Note** Importing software images from devices is not allowed.
not uploaded into the Catalyst Center repository,	only download the image,	**a.** Under **Image Name**, locate the image that you want to mark as standard. **b.** From the corresponding **Available for download** drop-down list for the image, choose **Download from Cisco.com**. **c.** In the **Download Image** dialog box, click **Save**. Under **Actions**, the software image download in-progress bar is displayed. This process might take some time. **Note** Importing software images from devices is not allowed.

Note If the image download fails, click **Show task** to view the **Recent Tasks** slide-in pane. From the **Task Status** drop-down list, choose **Failed**. Click **See why?** to view the failure details.

Step 5 If you want to download an add-on of the standard image, complete these steps:

a. Under **Image Name**, locate the software image with the add-on and verify that the image is marked as standard.

Note
- If the software image with the add-on that you want to download is not marked as standard, you must first mark that image as standard.
- The **Add-ons** column lists the number of add-ons for each software image.

b. Expand the standard image row.

The add-on is displayed in the expanded image row.

c. From the corresponding **Available for download** drop-down list for that add-on, choose **Download from Cisco.com**.

Note
- Subpackages are only downloadable.
- SMU, APSP, APDP, and PSIRT SMU upgrades for the base image are downloadable and can be marked as standard.

d. In the **Download Image** dialog box, click **Save**.

Re-expand the image row with the add-on to view the progress spinner under **Actions**. This process might take some time. When the download is completed, **Downloaded** is displayed under **Actions**.

Manage the standard software image

You can manage the software image that is marked as standard with or without conditions.

Before you begin

The software image must be marked as standard with or without conditions. For more information, see Mark a software image as standard, on page 545.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click **Devices**.

Step 3 Under **Device Family**, click the hyperlinked device family for which you want to manage its standard image.

Step 4 Manage the standard image with or without conditions using this table.

If you want to...	Then...
edit a standard software image with or without conditions,	**a.** Under **Image Name**, locate the standard image. **b.** From the corresponding **Marked as standard** or **Conditionally marked as standard** drop-down lists for the image, choose **Edit standard conditions**. **c.** In the **Mark as standard** slide-in pane, update the advanced settings and then click **Confirm**. • **Device role**: From the drop-down list, choose a role. • **Device tags**: From the drop-down list, check or uncheck the device tag check boxes.
unmark a software image as standard without conditions	**a.** Under **Image Name**, locate the standard image. **b.** From the corresponding **Marked as standard** drop-down list for the image, choose **Remove standard**. The image is now in the downloaded state. **Note** If the image is marked as standard with conditions, you must first mark it as standard without conditions (that is, remove the conditions). Then, you can unmark it as standard.
replace the standard software image,	When you mark a different software image as standard with or without conditions, the current standard image is replaced with the new one. For more information, see Mark a software image as standard, on page 545.

Configure an image distribution server

An image distribution server helps in the storage and distribution of software images. You can configure up to three external image distribution servers to distribute software images. You can also set up one or more protocols for the newly added image distribution servers.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

Step 2 In the **Image Distribution Servers** window, click **Servers**.

The table displays details about the host, username, SFTP, SCP, and connectivity of image distribution servers.

Step 3 Click **Add** to add a new image distribution server.

The **Add a New Image Distribution Server** slide-in pane is displayed.

Step 4 Configure these image distribution server settings:

- **Host**: Enter the hostname or IP address of the image distribution server.
- **Root Location**: Enter the working root directory for file transfers.

Note For Cisco AireOS Wireless Controllers, image distribution fails if the configured path is longer than 16 characters.

- **Username**: Enter a username to log in to the image distribution server. The username must have read/write privileges in the working root directory of the server.
- **Password**: Enter a password to log in to the image distribution server.
- **Port Number**: Enter the port number on which the image distribution server is running.

Step 5 Click **Save**.

Step 6 Because some legacy wireless controller software versions support only weak ciphers (such as SHA1-based ciphers) for SFTP, Catalyst Center should enable SFTP compatibility mode for SFTP connections from wireless controllers for software image management and wireless assurance. You can temporarily enable support for weak ciphers on the Catalyst Center SFTP server for up to 90 days. To allow weak ciphers:

a) Hover over the **i** icon next to the IP address of the SFTP server and click **Click here**.
b) In the **Compatibility Mode** slide-in pane, check the **Compatibility Mode** check box and enter a duration (from 1 minute to 90 days).
c) Click **Save**.

Step 7 (Optional) To edit the settings, click the **Edit** icon next to the corresponding image distribution server, make the required changes, and click **Save**.

Step 8 (Optional) To delete an image distribution server, click the **Delete** icon next to the corresponding image distribution server and click **Delete**.

Change the protocol order of an image distribution server

You can change the protocol order of an image distribution server. Protocol order helps in performing verification checks on the image distribution servers. By default, the software images are distributed using the first protocol in the protocol order.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

Step 2 In the **Image Distribution Servers** window, click the **Preferences** tab.

The default protocol order displays.

Step 3 In the Protocol Order area, click the **On/Off** protocol toggle button to enable or disable a protocol.

- HTTPS—Catalyst Center logs in to the device and uses the **copy https://<Catalyst-Center-IP-address>/<Catalyst-Center-image-path>** command using TLS 1.2 with the Catalyst Center certificate authority. For any issues, see Troubleshoot HTTPS Error in Cisco Catalyst Center for SWIM.
- SCP—Catalyst Center logs in to the device and uses the **SCP://sftpuser:randomised-password@<Catalyst-Center-IP-address>/<Catalyst-Center-image-path>** command. For any issues, you must open a TAC case.
- SFTP—Catalyst Center logs in to the device and uses the **SFTP://sftpuser:randomised-password@<Catalyst-Center-IP-address>/<Catalyst-Center-image-path>** command. For any issues, you must open a TAC case.

Note The HTTPS or SCP protocol must be enabled for image distribution. The SFTP protocol must be enabled for all protocol orders to support legacy devices.

If the HTTPS protocol is disabled or image distribution fails while using the HTTPS protocol, the software image is distributed using the SCP protocol.

Step 4 Drag and drop the protocols to change the protocol order.

Step 5 Click **Save**.

Add image distribution servers to sites

You can associate SFTP servers located in different geographical regions to sites, buildings, and floors. All the devices under the network hierarchy use the associated image distribution server during a network upgrade.

Before you begin

You must configure an image distribution server. See Configure an image distribution server, on page 548.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Servers**.

Step 2 Expand the **Image Distribution** area to select SFTP servers to act as image distribution servers.

Step 3 Check the **Add image distribution servers** check box to view the fields.

Step 4 From the **Primary** drop-down list, choose the image distribution server that you want to configure as primary.

Step 5 Click the + icon and from the **Secondary** drop-down list, choose the image distribution server that you want to configure as secondary.

Step 6 Click **Save**.

Provision a software image

Catalyst Center compares each device software image with the image that you have designated as standard for that specific device type. If there is a difference between the software image and the standard image, Catalyst Center specifies that the software image of the device is outdated. If this is the case, you can update the outdated software image.

Before pushing a software image to a device, Catalyst Center performs upgrade readiness prechecks on the devices, such as checking the device management status, disk space, and so on. If any prechecks fail, you cannot perform the software image upgrade. You need to correct any issues before you can upgrade the software image on the devices.

If all the prechecks succeed, you can distribute (copy) the new image to the device and activate it (that is, make the new image the running image). The activation of the new image requires a reboot of the device. Because a reboot might interrupt the current network activity, you can schedule the process for a later time.

After the software image is successfully upgraded, Catalyst Center performs upgrade postchecks, such as checking the CPU usage, route summary, and so on, to ensure that the state of the network remains unchanged.

Before you begin

- Make sure the device type has a designated standard image. See Mark a software image as standard, on page 545.
- To upgrade the software image immediately, you must disable the Automation Events for ITSM (ServiceNow) bundle. To access the bundle, choose **Platform** > **Manage** > **Bundles** > **Automation Events for ITSM (ServiceNow)**.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click the **Images** tab. Select the image to be upgraded and mark the image as standard. To mark the image, see Mark a software image as standard, on page 545.

Step 3 In the **Devices** tab, select the devices that need to be updated with the image and click **Update Devices**.

Alternately, you can go to the **Overview** tab and click **Schedule Update** in the **Image Update Tools** section. You are redirected to the Image upgrade workflow.

Step 4 The **Image Update** window opens which prompts you with instructions to configure the image update.

Step 5 In the **Task Name** window, enter a unique name for the update task and click **Next**.

Step 6 In the **Select Devices** window, select the location of the devices from the left panel. In the **Devices** section, check the checkboxes for the devices you want to schedule the image update and click **Next**.

Note If the prechecks succeed for a device, the **Outdated** link in the **Software Image** column has a green check mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link has a red check mark, and you cannot update the software image for that device. Click the **Outdated** link and correct the errors before proceeding. See List of Device Upgrade Readiness Prechecks.

Step 7 In the **Software Distribution Checks** window, you can enable pre-checks and post-checks for the software distribution and select the check order. After choosing the distribution checks, click **Next**.

Note If you associated the external image distribution server with a network hierarchy, the image distribution server distributes the image to all devices under the network hierarchy. See Add image distribution servers to sites, on page 550.

To select the validators that you want to run for the current workflow or add new custom checks, do these steps:

a) Hover your mouse over the information icon to view the validation criteria and the CLI commands that are used for the validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do these steps:

1. Click **add a custom check** to launch the **New Custom Check** window.
2. Enter the **Name** for the custom check.
3. From the **When** drop-down list, select **pre**, **post**, or both.
4. From the **Select a Test Device** drop-down list, select the device you want to check.
5. Click **Open Command Runner**, and enter the CLI commands.
6. Expand **Add Known Command-Patterns to Ignore During Checks** to add a command pattern that is used to ignore the matching output for the checks.

   To add a command pattern:

   - To create a new pattern, enter a desired name and string or pattern.
   - To use an existing pattern, click **most commonly used patterns**, select the desired pattern, and click **Add Selected**.
   - Click **Test All Patterns**.

7. Expand the **Additional Criteria** area.

   From the **Operation** drop-down list, select **Distribution**, **Activation**, or both.

8. From the **Device Series** drop-down list, select the desired device series and click **Save**.

Step 8 In the **Software Activation Checks** window, you can enable pre-checks and post-checks for the software activation and select the check order. After choosing the activation checks, click **Next**.

Step 9 In the **Device Activation Order** window, you can use filters to sort devices and arrange the order of their activation in parallel or sequentially. After sorting the devices, you can reorder them sequentially. Click **Next**.

Step 10 In the **Schedule Task and Clean Up** window, schedule these tasks:

- In the **Software Distribution** section, enable the checks for the software distribution.
- In the **Software Activation** section, select either **Now** or **Later** to schedule the update. If you select **Later**, configure the start date and time, and select the time zone for the update to start. By default, the time zone is set as the time zone of the selected site.
- Check the **Initiate Flash Cleanup After Activation** checkbox to store only the running image and remove all previous images saved on the device.

After configuring the settings, click **Next**.

Step 11 The **Summary** window shows the summarized data of the scheduled update. Review the details and if required, you can click **Edit** to modify the settings. Click **Submit**.

Import the ISSU compatibility matrix

In-Service Software Upgrade (ISSU) is a process that upgrades an image on a device with no or minimal service interruption. ISSU is supported only within or between long-lived releases, such as 17.3.x to 17.3.y or 17.3.x to 17.6.y. You can download and import the ISSU compatibility matrix that corresponds to the target release in Catalyst Center to upgrade devices with ISSU.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 Click the **Images** tab and then click **Import images**.

Alternately, click the **Overview** tab and click **Import Image** in the **Image Update Tools** section.

Step 3 In the **Import Image** slide-in pane, click the **Select ISSU compatibility matrix** radio button and click **Choose a file** to navigate to an ISSU compatibility matrix file stored locally.

Step 4 Click **Import**.

Step 5 Click **Show Tasks** to view the ISSU compatibility matrix file import status.



Note Starting with Catalyst Center 2.3.7, compatibility matrix files are automatically downloaded for standard-tagged images and the running images of ISSU-supported devices available in cisco.com.

Upgrade a software image with ISSU or xFSU

You can choose to upgrade the device using ISSU or xFSU. ISSU is designed for chassis-based switches with dual supervisors to provide near-zero downtime upgrades, while xFSU is optimized for stackable access switches like Catalyst 9300 to minimize downtime during upgrades by separating control and data plane reloads.

xFSU support is available for Catalyst 9300 Series device running version 17.18.2 or later.

Before you begin

- Before you upgrade a device using the ISSU or xFSU, you must import the ISSU compatibility matrix file. See Import the ISSU compatibility matrix, on page 553.
- To upgrade the software image immediately, you must disable the Automation Events for ITSM (ServiceNow) bundle. To access the bundle, choose **Platform** > **Manage** > **Bundles** > **Automation Events for ITSM (ServiceNow)**.

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 In the **Devices** tab, select the devices that need to be updated with the image and click **Update Devices**.

Alternately, you can go to the **Overview** tab and click **Schedule Update** in the **Image Update Tools** section. You are redirected to the Image upgrade workflow.

Step 3 The **Image Update** window opens which prompts you with instructions to configure the image update.

Step 4 In the **Task Name** window, enter a unique name for the update task and click **Next**.

Step 5 In the **Select Devices** window, select the location of the devices from the left panel. In the **Devices** section, check the checkboxes for the devices you want to schedule the image update and click **Next**.

Note If the prechecks succeed for a device, the **Outdated** link in the **Software Image** column has a green check mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link has a red check mark, and you cannot update the software image for that device. Click the **Outdated** link and correct the errors before proceeding. See List of Device Upgrade Readiness Prechecks.

Step 6 In the **Software Distribution Checks** window, you can enable pre-checks and post-checks for the software distribution and select the check order. After choosing the distribution checks, click **Next**.

Note If you associated the external image distribution server with a network hierarchy, the image distribution server distributes the image to all devices under the network hierarchy. See Add image distribution servers to sites, on page 550.

To select the validators that you want to run for the current workflow or add new custom checks, do these steps:

a) Hover your mouse over the information icon to view the validation criteria and the CLI commands that are used for the validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do these steps:

1. Click **add a custom check** to launch the **New Custom Check** window.
2. Enter the **Name** for the custom check.
3. From the **When** drop-down list, select **pre**, **post**, or both.
4. From the **Select a Test Device** drop-down list, select the device you want to check.
5. Click **Open Command Runner**, and enter the CLI commands.
6. Expand **Add Known Command-Patterns to Ignore During Checks** to add a command pattern that is used to ignore the matching output for the checks.

   To add a command pattern:

   - To create a new pattern, enter a desired name and string or pattern.
   - To use an existing pattern, click **most commonly used patterns**, select the desired pattern, and click **Add Selected**.
   - Click **Test All Patterns**.

7. Expand the **Additional Criteria** area.

   From the **Operation** drop-down list, select **Distribution**, **Activation**, or both.
8. From the **Device Series** drop-down list, select the desired device series and click **Save**.

Step 7 In the **Software Activation Checks** window, you can enable pre-checks and post-checks for the software activation and select the check order. Click **Next**.

Step 8 In the **Device Activation Order** window, you can use filters to sort devices and arrange the order of their activation in parallel or sequentially. After sorting the devices, you can reorder them sequentially.

Step 9 If you want to upgrade with ISSU, follow these steps:

a) Select the device that you want to upgrade with ISSU.

Note The **Update Image** column shows the ISSU validation status.

- **ISSU shown in amber**: ISSU validation failed because the selected image is not ISSU compatible.
- **ISSU shown in gray**: ISSU validation succeeded and the device supports ISSU.

b) From the **ISSU** drop-down list, select **Enable ISSU Upgrade**.
c) Click **Next**.

Step 10 If you want to upgrade with xFSU, follow these steps

a) Select the device that you want to upgrade with ISSU.

Note The **Update Image** column shows the XFSU validation status.

- **xFSU shown in amber**: xFSU validation failed because the selected image is not xFSU compatible.
- **xFSU shown in gray**: xFSU validation succeeded and the device supports xFSU .

b) From the **xFSU** drop-down list, select **Enable xFSU Upgrade**.
c) Click **Next**.

Step 11 In the **Schedule Task and Clean Up** window, schedule these tasks:

- In the **Software Distribution** section, enable the checks for the software distribution.
- In the **Software Activation** section, select either **Now** or **Later** to schedule the update. If you select **Later**, configure the start date and time, and select the time zone for the update to start. By default, the time zone is set as the time zone of the selected site.
- Check the **Initiate Flash Cleanup After Activation** checkbox to store only the running image and remove all previous images saved on the device.

After configuring the settings, click **Next**.

Step 12 The **Summary** window shows the summarized data of the scheduled update. Review the details and if required, you can click **Edit** to modify the settings. Click **Submit**.

List of device upgrade readiness prechecks

Precheck	Description
File transfer check	Checks if the device is reachable through HTTPS and SCP The default order of protocols is HTTPS first and then SCP. For Catalyst Center configured with FQDN, an error message is displayed if the name server associated with the device is unreachable.
NTP clock check	Compares device time and Catalyst Center time to ensure successful Catalyst Center certificate installation.
Flash check	Calculates the disk space required for upgrading to the standard image with add-on and performs flash clean up proactively before image distribution. If there is not enough disk space, a warning or error message is returned. For information about the supported devices for Auto Flash cleanup and how files are deleted, see Auto Flash Cleanup.
Config register check	Verifies the config registry value.
Crypto RSA check	Checks whether an RSA certificate is installed.
Crypto TLS check	Checks whether the device supports TLS 1.2.

Precheck	Description
Weak Crypto Check	Checks whether the device is configured with weak crypto like SNMP V3 user added with MD5 authentication. The image upgrade is blocked due to weak crypto for device with software image version 17.14 and later.
IP Domain name check	Checks whether the domain name is configured.
Startup config check	Checks whether the startup configuration exists for the device.
NFVIS Flash check	Checks whether the standard image is ready to be upgraded in the NFVIS device.
Service Entitlement check	Checks whether the device has a valid license.
Image Compatibility Check	Checks whether the standard image is compatible with the device.
Image Version Support	Checks whether the device is tagged with the compatible standard image version. If the tagged image version is below compatible version, it will fail.
ISSU Compatibility	Checks whether the matching compatibility matrix is available for the running image and standard image.
Extended Fast Software Upgrade (xFSU) Compatibility Check	Devices self-assess and report XFSU eligibility based on current configuration and state.

View image update status

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**.

Step 2 In the **Overview** tab you can view these updates:

- **Updates**: Shows the number of image updates that failed, in-progress, and are successful.
- In the **Image Update Tools** section, click **Check Update Status** to check the status of the image updates that are triggered. The **Devices Updates** slide-in pane shows the updates that are in-progress, waiting, terminated, successful, and failed.

  Click **Upcoming Tasks** to view the scheduled updates.
- The **Yet to be submitted Image Update flows** section shows the upcoming tasks that are yet to be submitted. You can click the ellipsis icon in this section and choose to resume or delete the task.

Step 3 In the **Devices** tab, select the devices for which tasks failed by checking check boxes and click **Retry** to retry the image update.

Step 4 The **Updates** tab shows the details of recent image updates that failed, are successful, are in-progress, and are scheduled. You can click the link to a task to view more information.

View image update workflow

Procedure

Step 1 From the main menu, choose **Provision** > **Software Image Management**. In the **Overview** tab, click **Schedule Update** in the **Image Update Tools** section.

Alternately, you can also choose **Workflows** > **Image Update**.

Step 2 In the **Task Name** window, enter a unique name for the scheduled update task and click **Next**.

Step 3 In the **Select Devices** window, select the location of the devices from the left panel. In the **Devices** section, check the checkboxes for the devices you want to schedule the image update and click **Next**.

Note If the prechecks succeed for a device, the **Outdated** link in the **Software Image** column has a green check mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link has a red check mark, and you cannot update the software image for that device. Click the **Outdated** link and correct the errors before proceeding. See List of Device Upgrade Readiness Prechecks.

Step 4 In the **Software Distribution Checks** window, you can enable pre-checks and post-checks for the software distribution and select the check order. After choosing the distribution checks, click **Next**.

Note If you associated the external image distribution server with a network hierarchy, the image distribution server distributes the image to all devices under the network hierarchy. See Add image distribution servers to sites, on page 550.

To select the validators that you want to run for the current workflow or add new custom checks, do these steps:

a) Hover your mouse over the information icon to view the validation criteria and the CLI commands that are used for the validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do these steps:

1. Click **add a custom check** to launch the **New Custom Check** window.
2. Enter the **Name** for the custom check.
3. From the **When** drop-down list, select **pre**, **post**, or both.
4. From the **Select a Test Device** drop-down list, select the device you want to check.
5. Click **Open Command Runner**, and enter the CLI commands.
6. Expand **Add Known Command-Patterns to Ignore During Checks** to add a command pattern that is used to ignore the matching output for the checks.

   To add a command pattern:

   - To create a new pattern, enter a desired name and string or pattern.

- To use an existing pattern, click **most commonly used patterns**, select the desired pattern, and click **Add Selected**.
- Click **Test All Patterns**.

7. Expand the **Additional Criteria** area.

   From the **Operation** drop-down list, select **Distribution**, **Activation**, or both.

8. From the **Device Series** drop-down list, select the desired device series and click **Save**.

Step 5 In the **Software Activation Checks** window, you can enable pre-checks and post-checks for the software activation and select the check order. After choosing the activation checks, click **Next**.

Step 6 In the **Device Activation Order** window, you can use filters to sort devices and arrange the order of their activation in parallel or sequentially. After sorting the devices, you can reorder them sequentially. Click **Next**.

Step 7 In the **Schedule Task and Clean Up** window, schedule these tasks:

- In the **Software Distribution** section, enable the checks for the software distribution.
- In the **Software Activation** section, select either **Now** or **Later** to schedule the update. If you select **Later**, configure the start date and time, and select the time zone for the update to start. By default, the time zone is set as the time zone of the selected site.
- Check the **Initiate Flash Cleanup After Activation** checkbox to store only the running image and remove all previous images saved on the device.

After configuring the settings, click **Next**.

Step 8 The **Summary** window shows the summarized data of the scheduled update. Review the details and if required, you can click **Edit** to modify the settings. Click **Submit**.

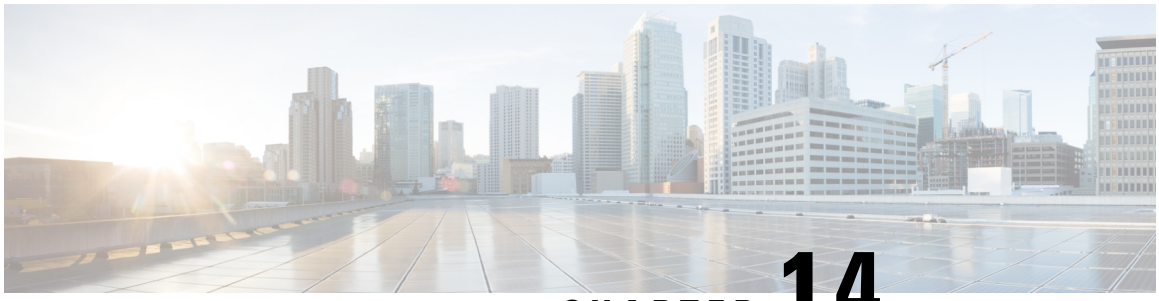
Auto flash cleanup

During the device upgrade readiness precheck, the flash check verifies whether there is enough space on the device to copy the new image. If there is insufficient space:

- **For devices that support auto flash cleanup**, the flash check fails with a warning message. For these devices, the auto cleanup is attempted during the image distribution process to create the sufficient space. As a part of the auto flash cleanup, Catalyst Center identifies unused .bin, .pkg, and .conf files and deletes them iteratively until enough free space is created on the device. Image distribution is attempted after the flash cleanup. You can view these deleted files in **Activities** > **Audit Logs**.

Note Auto flash cleanup is supported on all devices except Nexus switches and wireless controllers.

- **For devices that do not support auto flash cleanup**, the flash check fails with an error message. You can delete files from the device flash to create space before starting the image upgrade.



CHAPTER 14

Compliance Audit for Network Devices

- Compliance overview, on page 561
- Compliance categories, on page 562
- Monitor the network compliance, on page 567
- Manage configuration compliance, on page 569
- Configure compliance settings, on page 571
- View compliance summary, on page 572
- Manual compliance run, on page 574
- Generate a compliance audit report for network devices, on page 575
- Acknowledge compliance violations, on page 575
- Synchronize startup and running configurations of a device, on page 576
- Fix compliance violations, on page 577
- Compliance behavior after device upgrade, on page 578
- Limitations in CLI template compliance, on page 579

Compliance overview

Compliance in Catalyst Center enables administrators to efficiently monitor, assess, and manage the network's adherence to intended policies and configurations. With recent enhancements, the compliance feature now delivers a powerful, unified dashboard that provides a comprehensive, network-wide view of compliance status across all managed devices.

The Compliance Dashboard allows you to:

- **Network wide compliance summary:** View the health of your entire network from a single interface, with visual indicators for non-compliant devices and outstanding violations.
- **Review consolidated compliance categories:** Compliance data is organized into three primary categories—Configuration Compliance, Hardware and Software Compliance, and Vulnerability Compliance, making it easier to address specific issues.
- **Filter and analyze compliance data:** Quickly filter compliance results by site, device, or category, and drill down to see which devices are non-compliant and the specific reasons for violations.
- **Perform bulk compliance operations:** Efficiently acknowledge or unacknowledged multiple violations at once, either network-wide or for selected devices, streamlining large-scale compliance workflows.

- **Compare start-up and running configurations:** Use the dedicated view to compare startup and running configurations for selected devices, helping to identify and resolve discrepancies due to unsaved changes.

Compliance checks can be:

- **Automated:** Using the latest collected device data and real-time notifications from Catalyst Center services.
- **Manual:** Triggered on demand by the administrator for immediate assessment.
- **Scheduled:** Run automatically each day, with jobs ensuring that all devices are checked at least once every seven days.

Catalyst Center continues to report compliance only for the entities it actively manages, flagging the removal or modification of previously managed configuration elements. New out-of-band additions may not be reported for compliance until they are managed by Catalyst Center.

Compliance categories

The Compliance Dashboard categorizes device compliance violations into three primary types:

- **Configuration Compliance**: Tracks deviations from intended configuration settings, including network settings and startup versus running configuration discrepancies.
- **Hardware and Software Compliance**: Monitors software image versions and EOX (End of Life/End of Sale) status for hardware and modules.
- **Vulnerability Compliance**: Highlights devices affected by high-priority security advisories, allowing for prioritized remediation.

Compliance type	Compliance check	Compliance status
Configuration compliance		
Network Profile	Catalyst Center allows you to define its intent configuration using network profiles and push the intent to the device. If any violations are found at any time due to changes *in-band*, *out-of-band* or triggered by another catalyst center service, this check identifies, assesses, and flags it off. The violations are shown to the user under **Network Profiles** in the compliance summary window. **Note** Network profile compliance is applicable for routers, switches, and wireless controllers.	• Non-compliant: The device is not running the intent configuration of the profile. • Compliant: While applying a network profile to the device, the device configurations that are pushed through Catalyst Center are actively running on the device. • Error: The compliance could not compute the status because of an underlying error. For details, see the error log.

Compliance type	Compliance check	Compliance status
Network Settings	Catalyst Center allows you to define its intent configuration settings using network settings and to push the intent to the device. If any violations are found at any time due to out-of-band or any other changes, the compliance check identifies, assesses, and flags it off. You can view the violations under **Policy** in the **Configuration Compliance** window. **Note** Post UI upgrade, compliance for network settings will get triggered after 6 hours.	• Non-compliant: The device is not running the intent configuration. • Compliant: The intent configuration that was pushed is actively running on the device. • NA (Not Applicable): The device is not configured with network settings, or the device is not assigned to the site.
Rule-based compliance	Catalyst Center allows you to define custom compliance rules using CLI regular expressions. This provides flexibility to check for specific configuration patterns or values unique to your environment.	• Non-compliant: The device is not running the intent configuration. • Compliant: The intent configuration that was pushed is actively running on the device. • NA (Not Applicable): The device is not configured with network settings, or the device is not assigned to the site.
Startup versus Running Configuration	This compliance check helps in identifying whether the startup and running configurations of a device are in sync. If the startup and running configurations of a device are out of sync, compliance is triggered and a detailed report of the out-of-band changes is displayed. The compliance for startup vs. running configurations is triggered within 2 minutes of any out-of-band changes. **Note** Catalyst Center must be configured as a syslog server in the **Design** > **Network Settings** > **Telemetry** > **Syslogs** window for syslog-based collection to work.	• Non-compliant: The startup and running configurations are not the same. In the detailed view, the system shows different startup vs. running between or running vs. previous running. • Compliant: The startup and running configurations are the same. • NA (Not Applicable): The device, such as AireOS, is not supported for this compliance type.
Software and hardware compliance		

Compliance type	Compliance check	Compliance status
Software Image	This compliance check helps a network administrator to see if the tagged golden image in Catalyst Center is running on the device. It shows the difference between the golden image and the running image for a device. When there is a change in the software image, the compliance check is triggered immediately without any delay.	• Non-compliant: The device is not running the tagged golden image of the device family. • Compliant: The device is running the tagged golden image of the device family. • NA (Not Applicable): The golden image is not available for the selected device family.
		For Fabric Devices: • Non-compliant: The device is not running the tagged golden image of the device family, or the current software image version is not compatible for the network device. See the *Cisco SD-Access Compatibility Matrix* for the supported and recommended software image versions for your device. • Compliant: The device is running the tagged golden image of the device family, or the current software image version is compatible with the device. • NA (Not Applicable): The golden image is not available for the selected device family, or the device is not added to a fabric site.
	For Cisco Switch Stacks: Catalyst Center allows the network administrator to check if the tagged golden image is running on the primary switch and members of switch stacks.	• Non-compliant: The tagged golden image is not running on the primary switch and member switches. Also, the device will be non-compliant if golden tagging is not applicable for the device and the member switches are not running on the image version as that of the primary switch. • Compliant: The tagged golden image is running on the primary switch and member switches. Also, the device will be compliant if no golden tagging is applicable for the device and the member switches are running on the same image version as that of the primary switch. • NA (Not Applicable): The golden image is not applicable for the device, and the device is not a stacked switch.

Compliance type	Compliance check	Compliance status
EoX - End of Life	Catalyst Center allows you to check the compliance status for the hardware, software, and module of EoX devices. You can check the EoX compliance status from the **Compliance Summary** > **EoX - End of Life** tile. You can also view the EoX status of devices from the **Inventory** window, under the **EoX Status** column. **Note** To enable access to the EoX feature, authorize the CX Cloud Consent to Connect agreement through the Catalyst Center dashboard.	• Non-compliant: The device is non-compliant if the last date of support has ended. • Compliant: The device is compliant if the last date of support is in the future, including future-dated EOX findings.
Vulnerability compliance		
Critical Security (PSIRT)	This compliance check enables a network administrator to check whether the network devices are running without critical security vulnerabilities.	• Non-compliant: The device has critical advisories. A detailed report displays various other information. • Compliant: There are no critical vulnerabilities in the device. • NA (Not Applicable): The security advisory scan has not been done by the network administrator in Catalyst Center, or the device is not supported.
Intent compliance		
Fabric (SDA) This feature is in beta.	Fabric compliance helps to identify fabric intent violations, such as any out-of-band changes for fabric-related configurations. The fabric compliance status does not participate in determining the overall compliance status of the device, as the feature is in the beta stage.	• Non-compliant: The device is not running the intent configuration. • Compliant: The device is running the intent configuration.
SD-Access Unsupported Configuration This feature is in beta.	This compliance check enables you to identify unsupported SD-Access configurations. When a device is added to a fabric site, the compliance check is triggered immediately. To view the unsupported SD-Access configurations on a noncompliant device, click **Unsupported Configuration**. Under the **Unsupported Configuration** area, unsupported SD-Access configurations are highlighted in red. **Note** For devices that are not added to a fabric site, this compliance check is not used.	• Non-compliant: The device is running some configurations that are not supported for SD-Access. • Compliant: The device is running the configurations that are supported for SD-Access.

Compliance type	Compliance check	Compliance status
Policy Intent Compliance		
Application Visibility	Catalyst Center allows you to create an application visibility intent and provision it to a device through CBAR and NBAR. If there is an intent violation on the device, this check identifies, assesses, and shows the violation as compliant or noncompliant under the **Application Visibility** window. The automatic compliance checks are scheduled to run after 5 hours of receiving traps.	• Non-compliant: The CBAR/NBAR configuration is not running on the device. • Compliant: The intent configuration of CBAR/NBAR is running on the device.
Model Config	This compliance check enables the network administrator to check any mismatch from the designed intent of Model Config. The mismatch is shown under **Network Profile** in the **Compliance Summary** window.	• Non-compliant: There is a mismatch in the actual and intended value of the attributes in Model Config. • Compliant: The attributes in Model Config match the intended value.

Compliance type	Compliance check	Compliance status
CLI Template	Catalyst Center allows the network administrator to compare the CLI template with the running configuration of the device. The mismatch in the configuration is flagged. This mismatch is shown under **Network Profile** in the **Compliance Summary** window. To view the flagged CLI commands: 1. Click the **Network Profile** tile. 2. From the **CLI Deviations** area, choose the CLI template for which you want to view the mismatch. 3. The CLI commands are displayed in the **Realize Template** area, and the flagged commands are highlighted in red. **Note** Click the **View CLI Template Best Practices** link to view some of the best practices that must be used in a CLI template to minimize compliance issues. The running configuration for CLI template compliance is taken from the latest archive that is available for the device. Event-based archive takes at least 2 minutes to update after traps are received. For accurate results, we recommend that you wait at least 2 minutes before running compliance manually after a configuration change. Catalyst Center must be configured as a syslog server in the **Design** > **Network Settings** > **Telemetry** > **Syslogs** window for syslog-based collection to work. **Note** There are some limitations in CLI template compliance. See Limitations in CLI template compliance, on page 579.	• Non-compliant: There is a mismatch between the CLI template and the running configuration of the device. • Compliant: There is no mismatch between the CLI template and the running configuration of the device.

Monitor the network compliance

Use this dashboard to gain a high-level understanding of your network's compliance status. The dashboard is refreshed periodically; however, you can trigger a manual refresh to view the most current data.

Before you begin

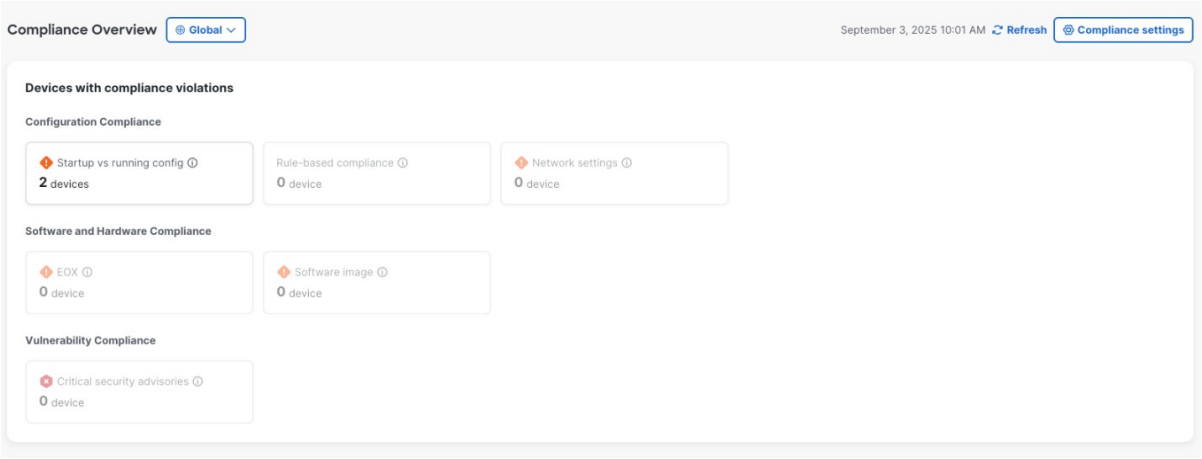
- Ensure you have the necessary administrative privileges.

Follow these steps to monitor the network compliance.

Procedure

Step 1 From the main menu, choose **Policy** > **Compliance Overview**.

Figure 23: Compliance Overview dashboard



Step 2 (Optional) Click the **Global** selector to filter the dashboard by a specific site.

In the **Devices with compliance violations** area, you can view the three primary categories of compliance violations:

- Configuration Compliance: Tracks deviations from established configuration baselines, including startup versus running configuration discrepancies, network profiles, and global settings.
- Software and Hardware Compliance: Monitors software image versions and EOX (End of Life/End of Sale) status for hardware and modules.
- Vulnerability Compliance: Highlights devices impacted by critical security advisories.

Step 3 Click on any compliance type to see a list of violations and non-compliant devices on the device table.

For more information on how to manage configuration compliance, see *Manage Configuration Compliance*.

Step 4 (Optional) Click **Refresh** to update the dashboard with the latest compliance data.

Step 5 Click **Compliance settings** in the top-right corner to open the settings window. You can enable or disable the violation check and set up customized compliance severity levels for different types of compliance violations.

The dashboard displays the current compliance status, allowing for targeted remediation of non-compliant devices.

Manage configuration compliance

Enable users to efficiently identify configuration drift, review active and acknowledged violations, and perform compliance audits to maintain network assurance..

Before you begin

- Ensure that you have the Super Admin role to modify compliance configuration.
- Set the dashboard scope to Global or a specific site to ensure the data reflects the desired network segment.
- Check the top-right corner of the dashboard to ensure the last compliance audit timestamp is current.

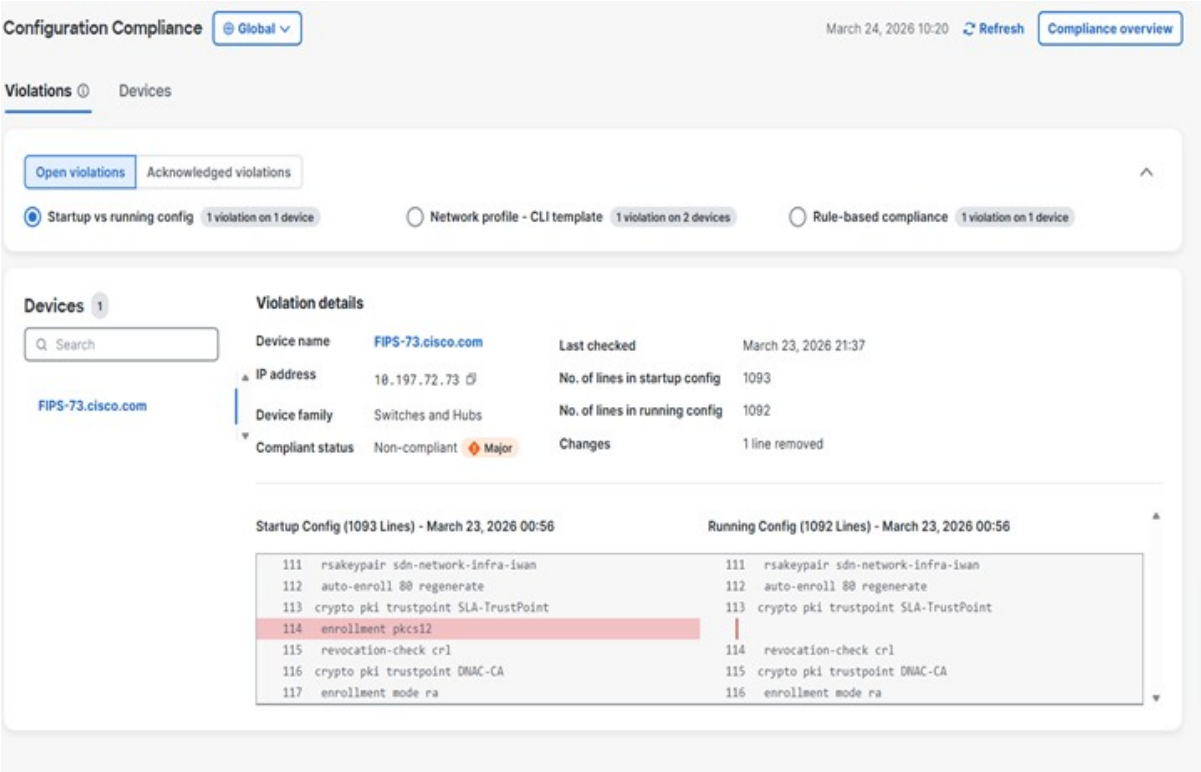
Use this procedure to analyze, acknowledge, and monitor configuration violations.

Procedure

Step 1 From the main menu, choose **Policy** > **Configuration Compliance**.

The compliance configuration dashboard appears.

Figure 24: Configuration Compliance



Step 2 Click the **Violations** tab to manage and view the violations.

a) Select the compliance type from the radio list such as **Rule-based compliance**, **Network profile - CLI template**, or **Startup vs running config**.

Step 3 Use the **Open violations** and **Acknowledged violations** toggle buttons to review the violations.

Option	Description
Open violations	Displays violations that are currently active and require attention.
Acknowledged violations	Displays violations that have been reviewed and acknowledged.

a) Review the violation details in the table for violation model name, affected devices, compliance type, sub-type, attribute, intended value, and actual value.
b) Click the value in the **On devices** column to view the devices affected by the violation.
c) Click **View details** in the **Intended value** column to compare the intended configuration with the actual device configuration.

Step 4 To manage compliance alert noise by acknowledging acceptable deviations or reverting previous acknowledgments do these:

a) Click the **Open Violations** tab.
b) Choose the violation and click **Acknowledge violations** on the top of the table.
c) To acknowledge the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Acknowledge violations**.
d) In the confirmation window, click **Confirm**. The violation is moved under **Acknowledged Violations** tab.
e) Click **Un-Acknowledge violations** to revert the status and return the items to the Open violations list.

Step 5 To monitor Device-level compliance to granular visibility into individual network nodes.

a) Click the **Devices** tab and select a compliance type focus to view and bulk manage the devices with compliance violations.

Step 6 Review the device table to identify:

a) Device name and IP address: The specific network node.
b) Compliance status: Use the drop-down list to filter the compliance status such as Compliant, Non- compliant, Error, NA, Not available, Aborted, In progress, Remediation in progress.
c) Severity: Use the drop-down list to filter the severity levels such as Critical, Major, Minor, and Informational
d) Config violations: Use the drop-down list to filter the types of configuration violations.

Step 7 (Optional) Select a device and click **Run compliance check** to trigger an immediate, manual audit of that device's configuration.

What to do next

- If a device remains non-compliant after a manual audit, click the hyperlinked Device name to open the Device 360 view.
- In Device 360 view, navigate to the Compliance tab to perform deep-dive troubleshooting and initiate configuration remediation.

Configure compliance settings

The primary purpose of configuring compliance settings is to establish a standardized framework for network health and security. By customizing these settings, administrators can:

- Enforce Organizational Standards: Ensure that all network devices adhere to predefined configuration, software, and vulnerability policies.
- Mitigate Risk: Identify and address non-compliant devices that may pose security threats or operational instability.
- Optimize Visibility: Tailor the compliance dashboard to focus on the metrics that matter most to your specific network architecture, reducing "noise" from irrelevant alerts.
- Automate Governance: Transition from manual auditing to automated, policy-driven monitoring, ensuring consistent oversight across the entire network infrastructure.

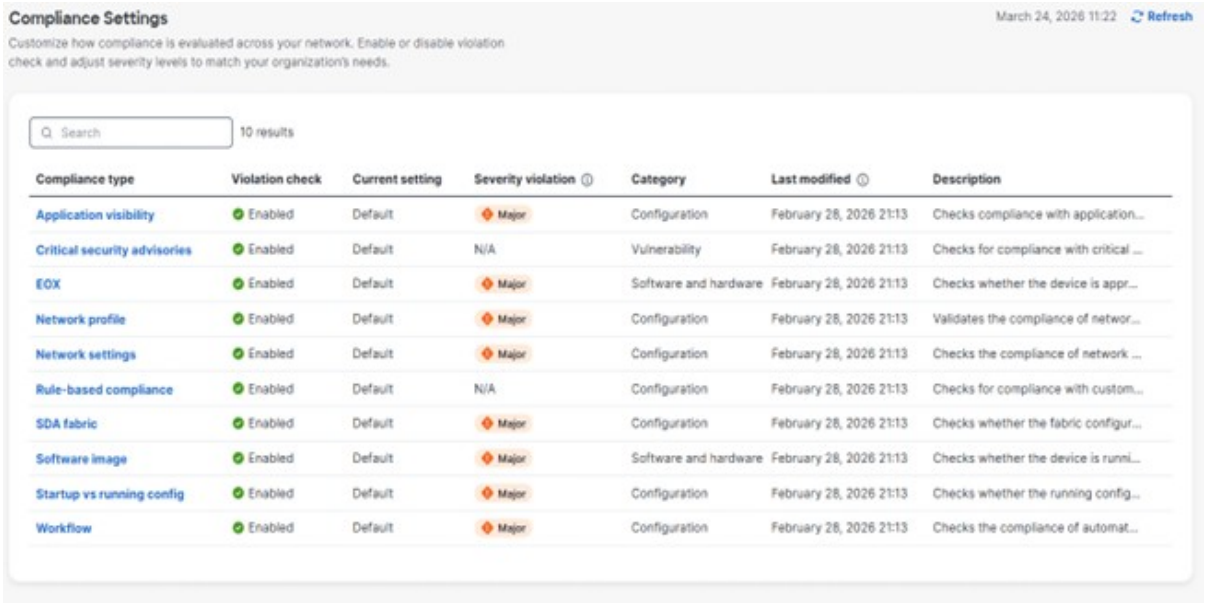
Before you begin

- Ensure you have the required administrative privileges to modify compliance settings.
- Understand that changes to these settings apply to all future compliance audits across the network.

Procedure

Step 1 From the main menu, choose **Policy** > **Compliance Settings**.

Figure 25: Compliance Settings dashboard



Step 2 (Optional) Use the Search box to locate a specific compliance type.

Step 3 Review the Compliance Settings table for each item:

- Violation check: Indicates if the check is Enabled or Disabled.
- Current setting: Displays the configuration status.
- Severity violation: Shows the assigned impact level.
- Category: Indicates the compliance area such as Configuration, Vulnerability, Software and hardware).
- Last modified: Displays the last modified time.
- Description: Description of the compliance.

Step 4 Click the hyperlinked **Compliance type** to enable or disable the violation check for the respective compliance types open the slide-in pane.

Step 5 In the configuration slide-in pane,

You can enable or disable the violation check. (Enabled by default.) If the violation check is enabled, you can customize its severity level to: Critical, Major (the default setting), Minor, and Informational (no violations).

a) Click **Edit** and toggle the Violation check to enable or disable the check. If you disabled a check, the corresponding category will no longer contribute to the non-compliant device count on the dashboard.
b) Adjust the **Severity** violation level.
   Options include:
   - **Critical**: For high-priority issues.
   - **Major (Default)**: The standard level of severity.
   - **Minor**: For lower-priority issues.
   - **Informational**: For status updates or non-critical logs.
c) Click **Save** to apply your changes.
d) If you wish to return all settings to their original state, click the **Reset to default** button.

View compliance summary

The inventory page shows an aggregated status of compliance for each device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The compliance column shows the aggregated compliance status of each device.

Step 2 Click the compliance status to launch the compliance summary window, which shows these compliance checks applicable for the chosen device:

- Startup versus Running Configuration

Catalyst Center allows you to view the details of the out-of-band configuration changes for Startup versus Running Configuration. Hover the cursor over the bubble in the **Change History** area to view the details.



These details are for out-of-band changes:

- Lines Added, Removed, Modified: Shows the number of lines that were added, removed, or modified.
- Triggered By: Displays the configuration change event. For information on events, see Configuration Drift of a Device.
- Terminal Name, Login IP, Username: Displays the users terminal name, login IP, and username.
- Config Method, Timestamp: Displays the configuration method and timestamp of the change done.

Note If the Config Method is memory, it indicates that the device self-generated the configuration.

- Rule- Based Compliance Policies
- Software Image
- Critical Security Vulnerability
- Network Profile
- Network Settings
- Fabric
- SD-Access Unsupported Configuration
- Application Visibility
- EoX - End of Life
- Cisco Umbrella

Note Network Settings, Network Profile, Fabric, SD-Access Unsupported Configuration, and Application Visibility are optional and display only if the device is provisioned with the required data.

Manual compliance run

You can trigger a compliance check manually in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 To run a bulk compliance check:

a) Choose all the applicable devices.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

Step 3 To run a per-device compliance check:

a) Choose the devices for which you want to run the compliance check.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

c) Alternatively, click the compliance column (if available) and then click **Run Compliance**.

Step 4 To view the latest compliance status of a device:

a) Choose the device and inventory. See Resynchronize device information, on page 182.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

Note

- A compliance run cannot be triggered for unreachable or unsupported devices.
- If compliance is not run manually for a device, the compliance check is automatically scheduled to run after a certain period of time, which depends on the type of compliance.
- CLI Template Compliance compares the realized templates against the running configuration of the device. The running configuration is taken from the latest archive that is available for the device.
- Event-based archive takes at least 2 minutes to update after traps are received. For accurate results, we recommend that you wait for at least 2 minutes before running compliance manually after a configuration change.
- Catalyst Center must be configured as a Syslog server in **Design** > **Network Settings** > **Telemetry** > **Syslogs** window for Syslog based collection to work.

Generate a compliance audit report for network devices

Catalyst Center allows you to retrieve a consolidated compliance audit report that shows the compliance status of individual network devices. With this report, you can get complete visibility of your network.

For more information, see "Run a compliance report" in the *Cisco Catalyst Center Platform User Guide*.

Acknowledge compliance violations

Catalyst Center lets you acknowledge less-important compliance violations of the device and opt-out the violations from the compliance status calculation. If required, you can also choose to opt-in the violation for the compliance status calculation.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Click the device name to open a dialog box that provides high-level information for that device. Click **View Device Details** link in the dialog box.
The device details window displays.

Step 3 In the left pane, choose **Compliance** > **Summary**.

Step 4 In the **Compliance Summary** window, click the compliance tile for which you want to acknowledge the violations.

You can view the information under **Open Violations** and **Acknowledged Violations** table, including:

- Model Name
- Attribute
- Status: This column shows one of the status states:
  - **Added**: The attribute is added in the device.
  - **Changed**: The intent value does not match the device value.
  - **Removed**: The intent is removed from the device.
- Intended Value: Shows the intended value as configured by Catalyst Center.
- Actual Value: Shows the value currently configured on the device.
- Action: Shows **Acknowledge** link for open violations and **Move to Open Violations** link for acknowledged violations.

To opt-out the violation from the compliance status calculation:

a) Click the **Open Violations** tab.
b) Choose the violation and click **Acknowledge** in the **Actions** column.
c) To acknowledge the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Acknowledge**.
d) In the confirmation window, click **Confirm**.
The violation is moved to the **Acknowledged Violations** tab.

To opt-in the violation for the compliance status calculation:

a) Click the **Acknowledged Violations** tab.
b) Choose the violation and click **Move to Open Violations** in the **Actions** column.
c) To move the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Move to Open Violations**.
d) In the confirmation window, click **Confirm**.
The violation is moved to **Open Violations** tab.

Step 5 To see a list of attributes that you opted out from the Compliance status calculation, click the **View Preference for Acknowledged Violations** link in **Compliance Summary** window.

Step 6 In the **Acknowledge Violation Preferences** slide-in pane, opt-in the attribute for the compliance status calculation:

a) Choose the attribute and click **Unlist** in the **Actions** column.
b) For bulk selection, check the check box at the top of the table, or choose multiple violations and click **Unlist**.

The **Models** tab shows attributes that are acknowledged for Model Config, Routing, Wireless, Application Visibility, or Fabric. Acknowledged templates are shown under the **Templates** tab.

Note

- In **Acknowledge Violation Preferences** window, a model with an empty (-) attribute means that the entire model, including its child attributes, are acknowledged.
- When a violation with the status, **Added** or **Removed** is acknowledged, Catalyst Center automatically acknowledges similar attributes and their child attributes.
- An acknowledged child attribute cannot be moved to open violations when a similar violation with the status, **Added** or **Removed** is overriding.

Synchronize startup and running configurations of a device

When there is a mismatch in the startup and running configurations of a device, you can do a remediation synchronization to match the configurations.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 To do a bulk remediation:

a) Choose all the applicable devices.
b) From the **Actions** drop-down list, choose **Compliance** > **Write Running Config to Startup Config**.

To do a per-device remediation:

a) Choose the devices for which you want to do a remediation synchronization.
b) From the **Actions** drop-down list, choose **Compliance** > **Write Running Config to Startup Config**.

Alternatively, click the link under **Compliance** column and then choose **Compliance Summary** > **Startup vs Running Configuration** > **Sync Device Config**.

Step 3 To view the remedial status of the device:

a) From the main menu, choose **Provision** > **Inventory**.

b) From the **Actions** drop-down list, choose **Compliance** > **Check Startup Config Write Status**.

Fix compliance violations

Catalyst Center maintains network compliance by automatically resolving both general configuration drift and violations identified by Rule-Based Compliance (RBC) policies. You can automatically push corrective CLI commands to non-compliant devices to bring them back into a compliant state.

A policy is eligible for remediation only if all violated conditions have a configured Fix CLI. All violated conditions have a Fix CLI. These are selected by default in the remediation. At least one violated condition lacks a Fix CLI. These policies are not eligible for remediation until the missing Fix CLI is added and a new compliance run is performed.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The compliance column shows the aggregated compliance status of each device.

Step 2 Click the compliance status to launch the **Compliance Summary** window.

Step 3 Click **Fix All Configuration Compliance Issues** link, at the top of the window.
The **Remediate** slide-in pane is displayed.

Note The link for fixing compliance violations is visible only if the supported category has violations. Otherwise, the link is not shown.

Step 4 In the **Remediate compliance** slide-in pane, review the violation categories for the network devices:

a) **Compliance Type**: Expand the compliance type to view the list of compliance **type** and **number of violations** aggregated count of open and acknowledged violations.

b) **Rule-based compliance**: Displays violations categorized by rule-based compliance policy. You can toggle between **Remediable violation** and **Non-remediable violation** tabs to view the **Policy name** and **Number of violations** for the remediable and non-remediable violations.

c) Click **Schedule the Fix**.

d) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 5 On the **Tasks** window, monitor the task deployment.

Note

- HA Remediation, Routing, Wireless Controller HA Remediation, Software Image, Security Advisories, and Workflow-related compliance issues are not addressed in this remediation fix. You can address these separately by using the actions in their respective sections.
- CLI template compliance has some limitations, because of which some CLI templates may remain non-compliant. For more information, see Limitations in CLI template compliance, on page 579.
- In Catalyst Center Release 2.3.7 and later, the intent is updated on Catalyst Center instead of pushing the configuration directly to the device for these changes:
  - For IPDT, if protocol endpoint is discovered.
  - For SNMP trap configuration, if SNMP user group change is detected from the system.

  IPDT configuration is pushed directly to the device for any device role change.

Compliance behavior after device upgrade

- A compliance check for all applicable devices (devices for which compliance never ran in the system) is triggered after successful device upgrade.
- Compliance calculates and shows the status of the devices in the inventory, except the Startup vs Running type.
- After upgrade, the Startup vs Running tile shows as NA with the text "Configuration data is not available."
- After a day of successful upgrade, a one-time scheduler runs and makes configuration data available for devices. The Startup vs Running tile starts showing the correct status (Compliant/Noncompliant) and detailed data.
- If any traps are received, the config archive service collects configuration data and the compliance check runs again.

Note In the upgrade setup, ignore any compliance mismatch for the **Flex Profile** interface. For the interface name, **1** maps to **management**.

Limitations in CLI template compliance

Catalyst Center allows you to compare a CLI template with the running configuration of the device, so as to identify any mismatch from the intent. Comparator engine limitations include:

- The CLI Template comparator supports use of uppercase letters for variables and values. But, you must avoid using uppercase letters for command keywords.
- The CLI Template comparator supports use of aliases.
- Avoid using abbreviated or shorthand commands, which are flagged as noncompliant.
- If a command is missing and it is at the section level, the section-level commands succeeding the missing command are also flagged. To avoid this problem, use indentation.

  For example, this CLI Template comparator output shows commands without indentation:

Realized template	Running configuration	Output

`#interface Vlan111`
`#description SVI interface kan-111`
`#ip address 111.2.3.4 255.255.255.0`
`#ip helper-address 7.7.7.8`
`#no mop enabled`
`#no mop sysid`
`#!`
	`#interface Vlan111`
	`# description SVI interface kan-111`
	`# ip address 111.2.3.4 255.255.255.0`
	`# ip helper-address 7.7.7.7`
	`# ip helper-address 7.7.7.8`
	`# no mop enabled`
	`# no mop sysid`
	`#!`
		These commands are marked as missing:
		
		`# ip helper-address 7.7.7.7`
		`# ip helper-address 7.7.7.8`
		`# no mop enabled`
		`# no mop sysid`

  This CLI Template comparator output shows commands with indentation:

Realized template	Running configuration	Output

`#interface Vlan111`
`# description SVI interface kan-111`
`# ip address 111.2.3.4 255.255.255.0`
`# ip helper-address 7.7.7.8`
`# no mop enabled`
`# no mop sysid`
`#!`
	`#interface Vlan111`
	`# description SVI interface kan-111`
	`# ip address 111.2.3.4 255.255.255.0`
	`# ip helper-address 7.7.7.7`
	`# ip helper-address 7.7.7.8`
	`# no mop enabled`
	`# no mop sysid`
	`#!`
		The comparator flags only the missing command:
		
		`#ip helper-address 7.7.7.7`

- Interactive and enable mode commands are not compared for compliance. You can use an alternative form of interactive commands by mentioning all the options and values with the commands.

  For example, if the template code is as follows, where **#ENABLE** and **#INTERACTIVE** mode command are given together, the commands are not compared.

```
#MODE_ENABLE
 #INTERACTIVE
    mkdir <IQ>Create directory<R>xyz
 #ENDS_INTERACTIVE
 #MODE_END_ENABLE
#end
```

- Avoid using ranges in commands, which are flagged by the comparator. Ranges must be used in expanded form.
- Overriding commands within the same template are flagged. You can avoid mismatch by enclosing the commands within *ignore - compliance* syntax, as shown in this example.

Realized template	Running configuration	Output

`#no banner motd #Welcome to Cisco .:|:.#`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	• This command is flagged as missing:
		`no banner motd #Welcome to Cisco .:|:.#`
		• This command is also marked as missing, because the running command is already compared with the preceding command.
		`banner motd #Welcome to Cisco .:|:.#`

To avoid mismatch:

Realized template	Running configuration	Output

`#! @start-ignore-compliance`
`#no banner motd #Welcome to Cisco .:|:#`
`#! @end-ignore-compliance`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	There is no mismatch, because the command enclosed in the syntax is not compared.

- For later releases of Cisco IOS XE, some default commands are shown only when **show run all** command is issued, instead of the **show run** command. Therefore, these commands do not appear in the running configuration and are flagged as noncompliant.

Note To ignore these default commands from compliance check, open a support case with the Cisco Technical Assistance Center (TAC).

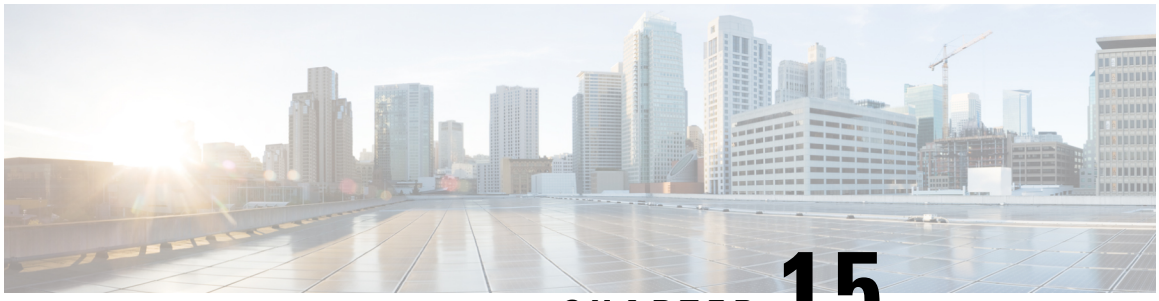
- Password-bearing commands are flagged by the comparator, because they are stored in encrypted form on the device.

Note You can avoid a mismatch for password-bearing commands and some default commands by enclosing the commands in this syntax:

```
! @start-ignore-compliance
! @end-ignore-compliance
```

Then, reprovision the template for the changes to appear.

To avoid a mismatch between the CLI template and the running configuration of the device, we recommend that you use commands similar to the running configuration.



CHAPTER 15

Run Diagnostic Commands on Devices

- Command Runner overview, on page 581
- Run diagnostic commands on devices, on page 581

Command Runner overview

The Command Runner tool allows you to send diagnostic CLI commands to selected devices. Currently, **show** and other read-only commands are permitted.

Run diagnostic commands on devices

Command Runner lets you run diagnostic CLI commands on selected devices and view the resulting command output. Command Runner supports only a subset of the shortcuts that are available as part of a standalone terminal.

Before you begin

Begin using Command Runner:

1. From the main menu, choose **System** > **Software Updates** > **Installed Apps**.
2. Find the **Command Runner** application and click **Install**.
3. After installation, run a Discovery job to populate Catalyst Center with devices. You are presented with a list of devices from which to run diagnostic CLI commands.

Procedure

Step 1 From the main menu, choose **Tools** > **Command Runner**.

Step 2 In the **Search** field of the **Command Runner** window, click the drop-down arrow to search by **Device IP** or **Device Name**.

Step 3 Choose a device or devices on which to run diagnostic CLI commands.

Device List displays your selection.

Step 4 (Optional) Select another device to add to the list. You can select up to 20 reachable devices.

Note Although the device list displays everything available in inventory, Command Runner is not supported for wireless access points and Cisco Meraki devices. If you choose an access point device or Cisco Meraki device, a warning message appears, stating that no commands will be executed on them.

Step 5 In the **Select/Enter commands** field, enter a CLI command and click **Add**.

Command Runner supports type ahead. As you begin typing, Command Runner displays the commands available for you to choose. You can also type a new, valid command.

Some commands, such as **ping** and **traceroute**, can be run in either interactive mode or noninteractive mode. However, Command Runner only supports noninteractive mode. Running commands in interactive mode may result in errors.

Step 6 Click **Run Command(s)**.

Note Command runner does not support parallel execution. Attempting to initiate a new command while one is already in progress will trigger an error message in the UI.

```
"A Command Runner session is already active for this device. Wait until the existing session is complete, then try again. You can continue to run commands on other devices. If this issue persists for an extended period, contact the Cisco TAC."
```

If successful, a `Command(s) executed successfully` message appears.

Some commands, such as **show tech**, require more time to execute in the command runner. Additionally, execution time depends on the device's response time and the size of the command output.

Step 7 Click the command displayed underneath the device to view the command output.

Note The complete command output is displayed in the **Command Runner** window. Any sensitive information, such as passwords, is masked in the command output.

Step 8 (Optional) Click **Export all CLI Output** to export the command output to a text file that you can save locally.

Step 9 Click **Go Back** to return to the previous window.

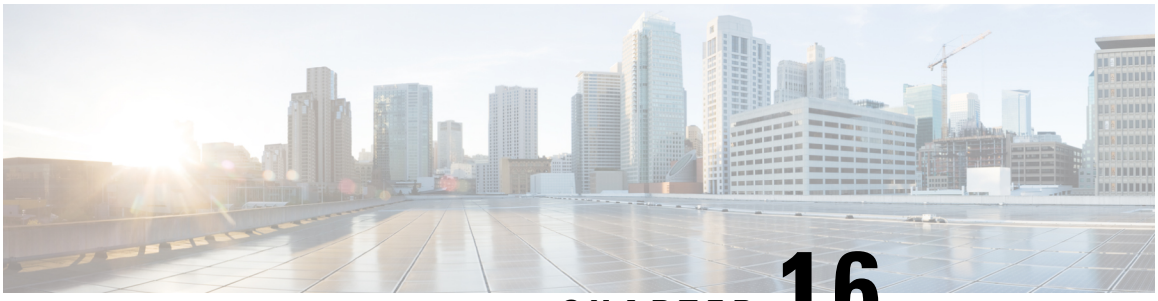
Note If necessary, click the **x** next to a device name to remove the device from the device list. Similarly, click the **x** next to a command to remove the command from the list.



PART V

Provision Your Network

- Onboard and Provision Devices with Plug and Play, on page 585
- Provision Wireless Devices, on page 617
- Provision a Routing Profile, on page 981
- Provision Firewall Profiles, on page 985
- Provision a LAN Underlay, on page 989
- Provision SD-Access LISP Fabric Network, on page 1005
- Provision Campus Networks, on page 1089
- Provision Services, on page 1113



CHAPTER 16

Onboard and Provision Devices with Plug and Play

- Plug and Play provisioning overview, on page 585
- Plug and Play provisioning prerequisites, on page 588
- Plug and Play deployment guidelines, on page 593
- View devices, on page 594
- Add or edit a device, on page 596
- Add devices in bulk, on page 597
- Register or edit a virtual account profile, on page 598
- Add devices from a Smart Account, on page 599
- Provision a device with Plug and Play, on page 601
- Delete a device, on page 614
- Reset a device, on page 614

Plug and Play provisioning overview

Plug and Play provisioning provides a way to automatically and remotely provision and onboard new network devices with minimal network administrator and field personnel involvement.

Using Plug and Play provisioning, you can:

- Provision devices by assigning a site, deploying site settings, installing a device software image, and applying a custom onboarding configuration.
- Plan devices before their installation by entering device information and choosing provisioning operations. When the device comes online, it contacts Catalyst Center and Plug and Play provisions and onboards the device automatically.
- Provision unclaimed network devices, which are new devices that appear on the network, without prior planning.
- Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal in a Cisco Smart Account to Plug and Play, so that all the devices appear in Catalyst Center.
- Display the detailed onboarding status of network devices.

These sections describe typical use cases and workflows for Plug and Play provisioning.

Planned provisioning

An administrator can plan the provisioning of a new site or other group of network devices.

Note The planned state for APs is for only claiming the APs using zero-touch provisioning (ZTP) when the APs contact Catalyst Center through Plug and Play. This planning isn't applicable for provisioning the APs via the **Provision** > **Inventory** option when the APs directly associate with the wireless controller.

The steps for planned provisioning include:

1. We recommend that you define the site within the network hierarchy. See Network hierarchy, on page 229.
2. Define the Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. Often, such templates aren't necessary unless you need to customize the day-zero configuration. See Create Templates to Automate Device Configuration Changes, on page 483.

Note Day-zero templates don't support Interactive commands.

3. Define network profiles for the types of devices that you are deploying. See Network profiles overview, on page 453.
4. We recommend that you define the device credentials (CLI and SNMPv2c/SNMPv3) for the devices that you're deploying. If you're using SNMPv2c, both Read and Write credentials must be provided.

Note Missing credentials will lead to the devices not being able to be added to the inventory after they are provisioned.

5. Ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository. See Import a software image, on page 539.
6. Add details about planned devices one at a time or in bulk with a CSV file. See Add or edit a device, on page 596 or Add devices in bulk, on page 597.
7. Devices boot up and are automatically provisioned.

Unclaimed provisioning

If a new network device is added to the network before it can be planned, it's labeled as an unclaimed device. An unclaimed device can be added manually by an administrator, or automatically through one of the discovery methods described in Plug and Play provisioning prerequisites, on page 588.

The steps for an administrator to provision the device include:

1. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View devices, on page 594.

2. Claim the device by assigning a site, image, configuration template, or profile. See Provision a device with Plug and Play, on page 601. You can also claim the device without assigning a site.

Note Global device credentials are required for devices with no site assigned. Global device credentials at site level are required for devices with sites assigned.

Cisco Smart Account synchronization and provisioning

Network devices can be automatically registered through a Cisco Smart Account with the Cisco Plug and Play Connect cloud service. An administrator can synchronize the device inventory from Cisco Plug and Play Connect to Catalyst Center Plug and Play, so that all the devices appear in Catalyst Center. These devices can then be claimed and provisioned.

1. Register a Smart Account and virtual account with which to synchronize. See Register or edit a virtual account profile, on page 598.
2. Synchronize the device inventory from the Smart Account. See Add devices from a Smart Account, on page 599.
3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View devices, on page 594.
4. Claim the device by assigning a site, image, configuration template, or profile. See Provision a device with Plug and Play, on page 601.
5. Devices boot up and are automatically provisioned.

Device claim and management scenarios

- **Claimed devices**
  - When a device is claimed and managed, PnP profiles are removed from the device.
  - The device will not contact PnP again only after a factory reset.
- **Unclaimed devices in inventory**
  - If a user tries to claim a device through PnP that is already in inventory, the claim is blocked.
  - Catalyst Center reads inventory notifications and updates PnP to prevent duplicate claims.
- **Factory reset devices**
  - If a managed device is factory reset, it moves to the unclaimed state.
  - Catalyst Center checks for inventory presence and blocks new claims if the device is still in inventory.

Plug and Play provisioning prerequisites

Before using Plug and Play provisioning, ensure you have access to the sites and devices where you want to provision, along with the necessary permissions to perform Plug and Play provisioning. For more information, see User profile roles and permissions, on page 23.

Ensure all device types meet the required prerequisites. Additionally, if you are deploying wireless or sensor devices, make sure those prerequisites are also met. Other prerequisites are optional, but if you choose to implement them, they must be completed before using Plug and Play to provision devices.

Prerequisites for all devices

Make sure all device types meet these prerequisites:

- Make sure devices can automatically discover the Catalyst Center controller in one of these ways:
  - DHCP: See DHCP controller discovery, on page 590.
  - DNS: See DNS controller discovery, on page 592.
  - Cisco Plug and Play Connect cloud service: See Plug and Play connect controller discovery, on page 592.
- Set the cisco.com credentials in the main Catalyst Center settings by using **System** > **Settings** > **Cisco.com Credentials**.

  If needed, set the Cisco Smart Account credentials in **System** > **Settings** > **Smart Account**.
- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in *Network Plug and Play Troubleshooting Guide for Cisco Catalyst Center*.

Prerequisites for wireless or sensor devices

In addition to the previous prerequisites, make sure any wireless or sensor devices meet these requirements:

- For wireless AP devices, ensure that the Cisco Wireless Controller that is managing the wireless APs has been added to the inventory, provisioned, and assigned to the site where the wireless APs are going to be assigned. This requirement is not needed for Mobility Express APs.
- For wireless AP devices, define the wireless radio frequency profiles. See Create a wireless radio frequency profile, on page 383. This requirement is not needed for Mobility Express APs.
- For Mobility Express APs, define an IP address pool and a management interface. See Configure IP address pools, on page 337.
- For ROW APs, we recommend that you create an AP profile with the necessary country code and configure custom site tags. See Configure additional settings for an AP profile for Cisco IOS XE devices, on page 431.
- For intent APs, you can configure the AP location for PnP onboarding in the **PnP AP Location** window using the **Configure AP Location** check box. This check box is unchecked by default. If necessary, check this check box to configure the site assigned during PnP claim as the AP location during PnP

onboarding. For more information, see "Configure AP location for PnP onboarding" in the *Catalyst Center Administrator Guide*.

- For sensors, ensure that the sensor is reachable through the Catalyst Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Catalyst Center; however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ASCII value "5A1D;B2;K4;I172.16.x.x;J80;", where 172.16.x.x is the virtual IP address of Catalyst Center associated with the enp9s0 interface.
- PnP supports DHCP option 43, DNS option, or devicehelper method for AP discovery. If an AP joins a wireless controller using DNS option, but DHCP option 43 is employed for PnP discovery, contention will occur.

Optional prerequisites for wireless controllers

Optional prerequisites that help to automate the Plug and Play provisioning process include:

- Define the site within the network hierarchy. See Network hierarchy, on page 229.
- Define the CLI and SNMP credentials for the devices. See Configure global device credentials, on page 323.



Note You can claim Cisco IOS XE wireless controllers using CLI, SNMPv2c, or SNMPv3 credentials. If you use SNMPv2c, provide both Read Only and Read Write credentials.

- Ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images. See Import a software image, on page 539.



Note The image deployment process used by Plug and Play during day-zero provisioning is not the same as that used when updating a device image later, which is described in Provision a software image, on page 551. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or post-checks done, as it is expected that devices are in the factory default state.

- Define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See Create Templates to Automate Device Configuration Changes, on page 483.



Note You can use the `ip http client source-interface` CLI command in the Onboarding Configuration template, which makes Catalyst Center use that IP address as the management IP address for the device, especially for the scenario of multiple IPs or VRFs.

- Define network profiles for the devices. See Network profiles overview, on page 453.

System certificate requirements for Plug and Play

The PnP discovery process requires a valid system certificate to facilitate the secure transition from HTTP to HTTPS. If the system certificate is misconfigured, PnP discovery will fail. To ensure successful device discovery, verify these requirements:

- Ensure that the system certificate contains all necessary Subject Alternative Name (SAN) fields, including the SAN IP and SAN FQDN.
- The FQDN configured in the DHCP Option 43 string must match the FQDN present in the system certificate.
- Ensure that all hostnames defined in the system certificate are resolvable via your DNS infrastructure.

If there is a mismatch between the certificate configuration and the address provided during discovery, the device will be unable to establish a secure connection, resulting in a discovery failure.

DHCP controller discovery

When a Cisco network device first starts up with no startup configuration, it attempts to discover the Catalyst Center controller by using DHCP Option 43.

The prerequisites for the DHCP discovery method include:

- New devices can reach the DHCP server.
- The DHCP server is configured with Option 43 for Cisco Plug and Play. When configuring DHCP Option 43, you can use either the Catalyst Center Enterprise IP or Enterprise Virtual IP (VIP) or the fully qualified domain name (FQDN). If using an FQDN, ensure that your DNS server is configured to resolve the hostname to the correct Catalyst Center cluster address.

  When the DHCP server receives a DHCP discover message from the device, with Option 60 containing the string “ciscopnp”, it responds to the device by returning a response that contains the Option 43 information. The Cisco Plug and Play IOS Agent in the device extracts the Catalyst Center controller IP address from the response and uses this address to communicate with the controller.



Note For lightweight APs, Option 60 doesn't contain the string `ciscopnp`. Instead, it contains the Vendor Class Identifier (VCI) of the lightweight AP. Make sure to set the DHCP server rules as needed so that Plug and Play can discover the lightweight AP. For more information, see Configure DHCP OPTION 43 for Lightweight Access Points.

DHCP Option 43 consists of a string value that is configured like this example on a Cisco router CLI that is acting as a DHCP server:

```
ip dhcp pool pnp_device_pool         <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0    <-- Range of IP addresses assigned to clients
default-router 192.168.1.1           <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80;"    <-- Option 43 string
```

The Option 43 string has components, delimited by semicolons, including:

- 5A1N;—Specifies the DHCP suboption for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2;—IP address type:
  - B1 = hostname
  - B2 = IPv4 (default)
- I*xxx.xxx.xxx.xxx*;—Enterprise IP or Enterprise VIP address or hostname of the Catalyst Center controller (following a capital letter i). While the Enterprise VIP configuration is optional for a single-node deployment, it is required for a three node cluster. In this example, the IP address is 172.19.45.222.
- J*xxxx*—Port number to use to connect to the Catalyst Center controller. You must use port 80 for HTTP.



Note After trusted certificate installation during PnP discovery, the device automatically switches to using port 443 for HTTPS.

- K4;—Transport protocol to be used between the device and the controller:
  - K4 = HTTP (default)
  - K5 = HTTPS
- T*TrustedCertificateBundleURL*;—Optional parameter that specifies the external URL of the trusted certificate bundle if it is to be retrieved from a different location than the default, which is the Catalyst Center controller, which gets the bundle from the Cisco InfoSec cloud (http://www.cisco.com/security/pki/). For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Tftp://10.30.30.10/ios.p7b

  If you are using trusted certificate security and you do not specify the T parameter, the device retrieves the trusted certificate bundle from the Catalyst Center controller.
- Z*xxx.xxx.xxx.xxx*;—IP address of the NTP server. This parameter is mandatory when using trusted certificate security to ensure that all devices are synchronized.

See the *Cisco IOS Command Reference* for additional details on DHCP configuration.

If DHCP Option 43 is not configured, the device cannot contact the DHCP server, or this method fails for another reason, the network device attempts discovery using DNS. For more information, see DNS controller discovery, on page 592.

If the Catalyst Center system certificate has an FQDN-only SAN field, you must edit the DHCP pool on the seed device to contain the Option 43 string with FQDN, B2 to B1, dns-server, and domain-name before starting PnP.

If the DHCP pool relies on Cisco switches or routers, it looks like this sample configuration:

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80;"
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS controller discovery

If DHCP discovery fails to get the IP address of the Catalyst Center controller, the network device falls back on the DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the controller, using the preset hostname pnpserver. The NTP server name is based on the preset hostname pnpntpserver.

For example, if the DHCP server returns the domain name “customer.com”, the network device constructs the controller FQDN of pnpserver.customer.com. It then uses the local name server to resolve the IP address for this FQDN. The NTP server name FQDN would be pnpntpserver.customer.com.

The prerequisites for the DNS discovery method include:

- New devices can reach the DHCP server.
- The Catalyst Center controller is deployed with the hostname “pnpserver”.
- The NTP server is deployed with the hostname pnpntpserver.

Plug and Play connect controller discovery

In situations where using the DHCP or DNS discovery methods is not an option, the Cisco Plug and Play Connect cloud service allows devices to discover the IP address of the Catalyst Center controller. When the network device boots up, if it cannot locate the controller through DHCP or DNS, then it tries Plug and Play Connect by contacting devicehelper.cisco.com to obtain the IP address of the appropriate controller that is defined for your organization. To secure the communications, the first thing that the device does when contacting Plug and Play Connect is to download and install the Cisco trusted certificate bundle.

These steps summarize how to use Cisco Plug and Play to deploy a Cisco network device by using Plug and Play Connect for discovery.

Before you begin

Cisco network devices are running Cisco IOS images that support Cisco Plug and Play and have connectivity to the Cisco Plug and Play Connect cloud service.

Procedure

Step 1 The network administrator configures the controller profile for the appropriate Catalyst Center controller for your organization by using Plug and Play Connect in the Cisco Smart Account web portal. For more information, see the Smart Account documentation in the web portal.

Step 2 If you order plug and play network devices through Cisco Commerce Workspace (CCW), these network devices are automatically registered with Plug and Play Connect as long as a Cisco Smart Account is assigned to the order and you include the NETWORK-PNP-LIC option for each device that you want to use with Cisco Plug and Play.

This option causes the device serial number and PID to be automatically registered in your Smart Account for plug and play. If you have specified a default controller, then the devices are automatically assigned to that controller when the order is processed.

Step 3 Alternatively, you can manually add devices in the Plug and Play Connect web portal.

Step 4 Register the Catalyst Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. See Register or edit a virtual account profile, on page 598.

This step is required if you order plug and play network devices through CCW and these network devices are automatically registered with Plug and Play Connect through your Smart Account.

Step 5 Synchronize the device inventory from the Smart Account in the Cisco Plug and Play Connect cloud portal to Catalyst Center Plug and Play.

Devices registered in the Plug and Play Connect web portal are synced to the controller and appear in the plug and play device list with a source of SmartAccount.

Step 6 Claim the newly synced devices. See Provision a device with Plug and Play, on page 601.

Step 7 The device installer installs and powers up the Cisco network device.

Step 8 The device discovers the Catalyst Center controller by querying the Plug and Play Connect service, identifies itself by serial number to Plug and Play in Catalyst Center, then is provisioned according to what was planned for it during the claim process.



Note The device will fail to contact Plug and Play Connect if the device cannot synchronize with the predefined NTP servers **time-pnp.cisco.com** or **pool.ntp.org**. To resolve this problem, either unblock NTP traffic to these two hostnames, or map these two NTP hostnames to local NTP server addresses on the DNS server.

Plug and Play deployment guidelines

Follow these recommendations when using Plug and Play for routers, switches, and wireless controllers:

- Device bring up order: In general, routing and upstream devices should be brought up first. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. The Plug and Play agent in a device attempts to auto-discover the Catalyst Center controller only during initial device startup. If at this time, the device cannot contact the controller, device provisioning fails, so upstream devices should be provisioned first.
- Cisco Router Trunk/Access Port Configuration: Typical branch networks include routers and switches. One or more switches are connected to the WAN router and other endpoints like IP phones and access points connect to the switches. When a switch connects to an upstream router, these deployment models are supported for Plug and Play:
  - Downstream switch is connected to the router using a switched port on the router. In this type of connection, the switched port on the router can be configured as a trunk or access port.
  - Downstream switch is connected to the router using a routed port on the router. In this case, the routed port can support multiple VLANs using sub-interfaces. During the Plug and Play process, the switch would automatically configure its port as a trunk port. In a large branch scenario, it becomes necessary to carry multiple VLANs between the router and the downstream switch. To support this use case, the switch must be connected to a routed port.
- Non-VLAN 1 configuration: Plug and Play supports devices using VLAN 1 by default. If you want to use a VLAN other than 1, adjacent upstream devices must use supported releases and you must configure

this global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnp startup-vlan** *x*. When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, the active interfaces on the upcoming Plug and Play device that are connected to the upstream device are changed to the specified VLAN. This guideline applies to both routers and switches and should be used only for trunk mode scenarios and not access mode.

View devices

You can view information about devices in the **Plug and Play** window.

In addition, you can perform several tasks from this window. For information, see these topics:

- Add or edit a device, on page 596
- Add devices in bulk, on page 597
- Add devices from a Smart Account, on page 599
- Provision a device with Plug and Play, on page 601
- Reset a device, on page 614
- Delete a device, on page 614

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

The **Plug and Play** window displays a table with device information, including:

Table 47: Device information

Column	Description
#	Row number.
Device Name	Hostname of the device. Click this link to open the device details window. A stack icon indicates a switch stack.
Serial Number	Device serial number.
Product ID	Device product ID.
IP Address	Device IP address.
Source	Source of the device entry: • User: User added the device through the GUI or API. • Network: Unclaimed device that has contacted the controller. • SmartAccount: Device was synced from a Smart Account.

Column	Description
State	• Unclaimed: Device successfully completed initialization and is ready to be claimed or put in Planned state. • Planned: User provided device configuration or provisioning parameters and the device is ready to be provisioned. • Onboarding: Device onboarding is in progress. • Provisioned: Device is successfully onboarded and added to inventory. For APs and sensors, the state changes to Provisioned after the device is successfully assigned to a wireless controller. • Error: Device had an error and could not be provisioned.
Onboarding State	Onboarding state of the device: • Not Contacted: Device has not called in. A user might have added or reset the device. • Connecting: Device called in. • Initializing: Executing system workflow. Basic device information is collected. Stack license and version mismatches are corrected. • Initialized: System workflow completed. • Executing Workflow: Any tasks that are selected during the claim are applied in this state. Stacks support renumbering and license update based on the product and image version. • Executed Workflow: User workflow completed. • Connection Error: Could not install certificates to secure a connection. • Authentication Error: Could not verify the SUDI certificate. • Authorization Error: Could not verify the user-provided SUDI serial number. • Initialization Error: Error executing system workflow. • Workflow Execution Error: Error executing user workflow. • Executing Reset: Executing reset workflow. You must manually reset the errored device, which reloads the device. • Reset Execution Error: Error executing reset workflow. Click the progress bar to go to the device history.
Site	Site with which the device is associated.
Last Contact	Last date and time the device contacted Plug and Play.
Smart Account	Cisco Smart Account with which the device is associated.
Virtual Account	Virtual Account (within the Cisco Smart Account) with which the device is associated.
Created	Date and time when the device was added to Plug and Play.

The Device table displays the information shown in the table for each device. Some of the columns support sorting.

Note

- Certain columns, such as **Device Name** and **Serial Number**, are displayed in the **Default** focus view.
- You can customize the **Devices** table to display or hide columns. Click the settings icon ( ) to display the **Table Settings** slide-in pane, and from the **Edit Table Columns** tab, choose which columns to display or hide. Click **Apply** to save the changes.

Step 2 From the **Plug and Play** window, you can control the display of device information in these ways:

- To sort the rows in ascending or descending order, click any column header with a carrot arrow icon .
- To display devices in a particular state, from the **Device Status** filter, choose **Unclaimed**, **Error**, **Provisioned** or **All**.
- To focus the view, from the **Focus** drop-down list, choose **Default** or **All**.
- To change when table information is refreshed, click the **Auto-Refresh** drop-down list and choose the desired auto-refresh time. By default, the devices table refreshes every 30 seconds.
- To find specific devices, use the **Filter** or **Find** option.
- To view device details, click the name of a device.

  To view additional details, from the window that opens, click the **Details**, **History**, or **Configuration** tabs. For a switch stack, you can also click the **Stack** tab. Some tabs have additional links that you can click for even more information.

Note To delete the stack member from a switch stack, under the **Stack** tab, check the check box next to the desired member and click **Delete Member**.

Add or edit a device

This procedure shows how to add or edit a device from the Plug and Play Devices list. Alternatively, you can edit a device from the device details window by clicking **Edit**.

Table 48: Device fields

Field	Description
Serial Number	Device serial number (read only if you are editing a device).
Product ID	Device product ID (read only if you are editing a device).
Device Name	Device name.

Field	Description
Enable SUDI Authorization	Enables secure unique device identifier (SUDI) authorization on devices that support it. When enabled, when a device attempts to connect to a Plug and Play server, the server compares the serial number on the SUDI certificate with the user-provided serial number. When the serial numbers match, the device is verified and connects to the Plug and Play server.
SUDI Serial Numbers	Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). Enter one or more comma-separated SUDI serial numbers in this field when adding a device that uses SUDI authorization. This field appears only if **Enable SUDI Authorization** is checked.
This Device Represents a Stack	Device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches.

Before you begin

If the device requires credentials, be sure that the global device credentials are set in the **Design** > **Network Settings** > **Device Credentials** page. For more information, see Add global CLI credentials, on page 323.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Add or edit a device:

- To add a device, click **Add Devices** and then click **Single Device**.
- To edit a device, check the check box next to the name of the device you want to edit and choose **Actions** > **Edit** in the menu bar above the device table. The **Edit Device** dialog displays.

Step 4 Set the fields as needed, referring to the preceding table for more information.

Step 5 Save the settings by doing one of these tasks:

- If you are adding a device and will claim it later, click **Add Device**.
- If you are adding a device and want to claim it immediately, click **Add + Claim**. For more information on claiming a device, see Provision a device with Plug and Play, on page 601.
- If you are editing a device, click **Edit Device**.

Add devices in bulk

This procedure shows how to add devices in bulk from a CSV file.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 Click **Add Devices**.

The **Add Devices** dialog displays.

Step 3 Click **Bulk Devices**.

Step 4 Click **Download File Template** to download the file template.

See the file template for information on which fields are mandatory and optional for different devices.

Step 5 Add the information for each device to the file and save the file.

Based on the device type, enter data in the mandatory fields.

Note If sites added through a file template are not present in the network hierarchy, they are removed.

For wireless controllers, Catalyst Center processes the data based on the IP address type: IPv4 address, IPv6 address, or both.

Step 6 Upload the CSV file using one of these options:

- Drag and drop the file into the drag-and-drop area.
- Click **Choose a file**, browse to the location of the CSV file, and click **Open**.

Step 7 Click **Import Devices**.

The devices in the CSV file are listed in a table.

Step 8 Check the box next to each device to import, or click the check box at the top to select all devices.

Step 9 Add the devices by doing one of these tasks:

- To add the devices and claim them later, click **Add Devices**.
- To add the devices and claim them immediately, click **Add + Claim**. For more information on claiming a device, see Provision a device with Plug and Play, on page 601.

Register or edit a virtual account profile

For redirection services, in a Cisco Smart Account, register Catalyst Center as a controller for Cisco Plug and Play Connect. This lets you add the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco Plug and Play in Catalyst Center.

You can register a Smart Account, virtual account, and the relevant server profile information with the Plug and Play system and database. The devices in the registered virtual account are synchronized with the Plug and Play database.

Table 49: Virtual Account Fields

Option	Description
Select Smart Account	Cisco Smart Account name.
Select Virtual Account	Virtual account name. Virtual accounts are subaccounts within a Cisco Smart Account.
IP or **FQDN**	**IP**: IPv4 address, IPv6 address, or both types of IP addresses for this Catalyst Center controller. **FQDN**: The fully qualified domain name for this Catalyst Center controller.
Profile Name	Controller profile name.
Use as Default Controller Profile	*Default controller profile* means that any new device that is added to a virtual account, or any existing device that doesn't have a default controller assigned, will be assigned to this redirection profile.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **PnP Connect**.

Step 2 View the virtual accounts in the table.

The table lists all of the registered Plug and Play Connect virtual account profiles.

Step 3 Either register or edit a virtual account profile:

- To register a virtual account, click **Register**. The Register Virtual Account pane is displayed.
- To edit a registered virtual account profile, click the radio button next to the name of the profile that you want to edit and click **Edit Profile**. The Edit Profile pane is displayed.

Step 4 Set the fields as needed.

Step 5 Save the settings by doing one of these tasks:

- If you are registering a new virtual account profile, click **Register**.
- If you are editing a virtual account profile, click **Save**.

What to do next

Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Catalyst Center Plug and Play. For more information, see Add devices from a Smart Account, on page 599.

Add devices from a Smart Account

This task allows you to synchronize the device inventory from a Smart Account in the Cisco Plug and Play Connect cloud portal to Catalyst Center Plug and Play.

The virtual accounts table displays information for each profile, including.

Table 50: Virtual accounts information

Column	Description
Virtual Accounts	Virtual account name
Smart Accounts	Smart account that the virtual account is associated with
Profile	Profile name
Controller	Controller IP address

Before you begin

Before you can synchronize the device inventory from the Cisco Plug and Play Connect cloud portal, you must register a virtual account. See Register or edit a virtual account profile, on page 598. You can go directly to the PnP Connect settings page by clicking the **PnP Connect** link in the **Add Devices** > **Smart Account Devices** dialog.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 Click **Add Devices**.

Step 3 Click **Smart Account Add** to open the **Add Devices from a Smart Account** slide-in pane.

Step 4 If you have already configured the cisco.com user, skip ahead to Step 5. If you haven't, complete these steps:

a) Open an Incognito/private window in your browser (to avoid using previously cached credentials).

b) Open another Catalyst Center GUI instance and log in.

c) Open another instance of the **Add Devices from a Smart Account** slide-in pane.

d) Complete one of these tasks:

If you...	Then...
completed a fresh installation of Catalyst Center 2.3.7.9,	configure a new cisco.com user by clicking the **Add** link in the **Cisco.com ID** field.
upgraded to Catalyst Center 2.3.7.9 and want to use the same cisco.com user that was configured previously,	reauthenticate that user by clicking the **Re-Authenticate** link in the **Cisco.com ID** field.
upgraded to Catalyst Center 2.3.7.9 and don't want to use the same cisco.com user as before,	delete the old cisco.com user and then configure a new one. 1. Click the **Delete** link in the **Cisco.com ID** field. 2. Confirm the operation by clicking **Delete** in the resulting dialog box. 3. Click the **Add** link in the **Cisco.com ID** field.

e) In the **Information** pop-up window, check one or both of these check boxes and then click **Authenticate**:

- (Mandatory) **I am in private or incognito mode**
- (Optional) **Save credentials**

f) In the **Activate your device** pop-up window, confirm that an activation code is displayed and then click **Next**.
g) In the **Log in** pop-up window, enter the cisco.com user's email address and then click **Next**.
h) In the **Verify with your password** pop-up window, enter the cisco.com user's password and then click **Verify**.

The **Device activated** pop-up window appears.

i) Close the **Device Activated** pop-up window.
j) Refresh the **Plug and Play** window, then click **Add Devices** > **Smart Account Add** to reopen the **Add Devices from a Smart Account** slide-in pane.
k) In the **Cisco.com ID** field, confirm that the email address you entered for the user displays. Also confirm that you see the **Change** link.

Step 5 Choose the Smart Account and virtual account that you want to register with Plug and Play.

If you need to register a PnP Connect virtual account profile, click the **PnP Connect** link. If you want to change the Cisco ID, click the **Not me?** link.

Step 6 From the Devices table, choose the devices that you want to add, and then click **Add Devices**.

Added devices appear in the Plug and Play Devices table with the source set to SmartAccount.

What to do next

Claim the newly added devices. For more information on claiming a device, see Provision a device with Plug and Play, on page 601.

Provision a device with Plug and Play

When you claim a device, the process of provisioning it begins. When a device is provisioned, Catalyst Center does these actions:

1. Deploys an image to the device.
2. Deploys system configuration CLI commands that configure these settings:
   - Device credentials (CLI and SNMP)
   - Enable SSH v2 and SCP server
   - Disable HTTP and HTTPS servers
   - For switches, vtp mode transparent is enabled
3. Deploys a device onboarding configuration template that corresponds to the type of device:
   - For wired devices, Catalyst Center deploys the onboarding configuration (day-zero) template that you defined.
   - For wireless devices, Catalyst Center deploys a configuration based on the network profile assigned to the site.

If your onboarding configuration template has any of the same system configuration CLI commands, the system configuration CLI commands are overridden, because the onboarding configuration template is applied to the device after the system configuration CLI commands.

4. Deploys Application Quality of Service (QoS) policy on the wired devices, if you configure QoS policy on the site to which the device is provisioned. For more information, see Create an application policy, on page 1231.
5. Pushes the NETCONF configuration on port 830 during device onboarding. The NETCONF port information is saved in the global credentials and network settings.

Note

- If NETCONF is pushed through incorrect port instead of the standard port 830, the device successfully completes onboarding but cannot be added to the inventory.
- If the device isn't assigned to a site during the claiming process, NETCONF isn't configured on the device.
- Automatic NETCONF enablement support is available for only:
  - Cisco Catalyst 9000 Series switches running Cisco IOS XE Release 17.3 or later and
  - Cisco Catalyst 9800 Series Wireless Controllers.

6. Application Telemetry and Controller-Based Application Recognition (CBAR) is enabled on the applicable network devices.
7. Adds the device to the inventory.
8. The PnP label trustpoint is removed automatically after the device successfully completes day-0 onboarding, is in managed state in the inventory, and is assigned to a site.

Note When Device Controllability is enabled for a device (it's enabled by default), additional configurations are pushed to the device when it's added to the inventory or assigned to a site. For more information, see the Device Controllability section in the *Cisco Catalyst Center Administrator Guide*.

When you claim a device that has not yet booted for the first time, the device is automatically provisioned when it boots up. This process is referred to as device *planning*.

The procedure for provisioning a device depends on the type of device:

- Switches and routers: See Provision a switch or router device, on page 602
- Cisco Wireless Controllers, APs, and sensors: See Provision a wireless controller, on page 606

Provision a switch or router device

This procedure shows how to claim a device from the **Plug and Play Devices** list. Alternatively, you can claim a device from the device **Details** window by clicking **Claim**.

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see Plug and Play provisioning prerequisites, on page 588.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

From the **Focus** drop-down list, choose **Default** or **All** to view the devices.

By default, the devices table is refreshed every 30 seconds. Click the **Auto-Refresh** drop-down list and choose a refresh time.

Use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to the device or devices that you want to claim.

Step 4 Choose **Actions** > **Claim** in the menu bar above the device table.

Step 5 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.

b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, choose a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Assign this Site to Other Devices**, choose the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

Note If you do not assign a device to a site, you must choose a template for the device in Step 6, on page 603.

c) Click **Next**.

Step 6 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and proceed to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Image**: From this drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.

Note If the device software image version or golden tagged version is 17.14.1 or later, the device claim is blocked if the selected site is configured with MD5 authentication for SNMP credentials.

If a golden image is not available, and the images are tagged with a specific device role (such as Border, Core, and so on) for this device type in the image repository, the drop-down list displays the available images.

To claim the device, you must also configure SHA authentication for SNMP credentials, or the software image version must be earlier than 17.14.1. For information on how to configure SHA authentication, see Edit global device credentials, on page 335.

- **Template**: From this drop-down list, choose an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

Note If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

- **Apply the PKCS12 device certificate on the device**: Check this check box to deploy a PKCS12 certificate to the device. This option is available only for routers.
- **RTU License Level**: From this drop-down list, choose **Lanbase** or **IP Services**. This option is available only for Cisco Industrial Ethernet (IE) 4000 Series and 5000 Series switches.
- **Select a Cabling Scheme**: From this drop-down list, choose the stack cabling scheme, if you want to renumber the stack.

  This item appears only for switches that support stacking, and only if they are connected, as shown in one of these cabling schemes.

Figure 26: Cabling schemes



- **Select a Top of Stack Serial Number**: The top-of-stack serial number autopopulates with the user-entered stack member serial number. If you don't want to use the autopopulated serial number, click the serial number, and in the **Select a Top of Stack Serial Number** field, click the drop-down arrow. Click the **X** icon to deselect the serial number.

  This option appears only for switches that support stacking, and only if they are connected as shown in the cabling schemes image.

  For a *planned device*, the top-of-stack serial number is set as the default. If necessary, you can specify a different serial number.

  For an *unclaimed device*, the top-of-stack serial number is not set as the default. Choose the top-of-stack serial number from the drop-down list.

- **Select a License Level**: From this drop-down list, choose the stack license level. Click the **X** icon to deselect the license level.

  This item displays only for switches that support stacking.

c) Click **Save**.

d) From the **Clear Configuration** drop-down list, choose any of these options:

- **Clear Device Certificates**: Choose this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Choose this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates**: Choose this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Choose this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

e) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon and choose **Apply Image to Other Devices** or **Apply Template to Other Devices**.

For stacked devices, you can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

f) If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.

g) After you have configured all the devices, click **Next**.

Step 7 To configure template parameter values for all the devices in bulk, skip to the next step. To configure template parameter values for devices one at a time, from the **Provision Templates** window:

a) Click the name of the device that you want to configure.

b) If the device was assigned a configuration template, specify the values for the parameters that were defined in the template.

Enter the values for each parameter in the fields for each device. A red asterisk indicates a required field.

c) If you want to copy the running configuration to the startup configuration on the selected device, check the **Copy running config to startup config** check box.

d) If you selected multiple devices to provision, click the next device in the list at the left side of the window and enter the parameter values, until you have done this for all the devices.

e) Click **Next**.

Step 8 To specify parameter values for all the devices in bulk, in the **Provision Templates** window:

a) Click **Export** to save the CSV template file.
b) Add the values for each of the parameters to the file and save the file.
c) Click **Import**.
d) Drag and drop the file to the drag-and-drop area, or click "**click to select**" and select the file.
e) Click **Import**.
f) Click **Next**.

Step 9 In the **Summary** window, view details about the devices and their configuration preview status.

Step 10 Verify the **Day-0 Config** column for each device to see whether the configuration preview succeeded.

If the preview shows an error, click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed.

To avoid provisioning errors, resolve issues, if any, before claiming the device. You may need to go back to the **Provision Templates** step and change the parameter values, and the template, revisit the **Design** area to update network design settings, or resolve network connectivity issues, if any.

After you resolve the problem, return to the **Day-0 Config** column, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.

Step 11 Click a link in the **Day-0 Config** column to see more information about the device, its configuration, and configuration preview errors, if any.

Step 12 Click **Claim**.

Step 13 In the confirmation dialog box, click **Yes** to claim the devices.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see Complete the provisioning process, on page 613.

Provision a wireless controller

This procedure explains how to claim a wireless controller from the Plug and Play Devices list. Alternatively, you can claim a device from the device **Details** window by clicking **Claim**.

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see Plug and Play provisioning prerequisites, on page 588.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the search bar to find specific devices.

Step 3 Check the check box next to the device or devices that you want to claim.

Step 4 From the menu bar above the device table, choose **Actions** > **Claim**.

Step 5 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.

b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, select a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon and select **Assign this Site to Other Devices**, select the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

If the wireless network profile associated with the assigned site has an onboarding template, Catalyst Center uses this template for PnP onboarding. For more information, see Add templates to a network profile, on page 465.

c) Click **Next**.

Step 6 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and continue to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Image**: From this drop-down list, select a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.

Note If the device software image version or golden tagged version is 17.14.1 or later, the device claim is blocked if the selected site is configured with MD5 authentication for SNMP credentials.

To claim the device, you must also configure SHA authentication for SNMP credentials, or the software image version must be earlier than 17.14.1. For information on how to configure SHA authentication, see Edit global device credentials, on page 335.

- **Template**: From this drop-down list, select an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

Note If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

For more information about onboarding APs for non-intent-based network deployments, including Assurance use case and Per-Device Configurations, see Onboard APs using PnP for non-intent-based deployments, on page 1448.

- **Catalyst Wireless LAN Controller Settings**: For a Cisco Catalyst 9800 Series Wireless Controller, enter data in the required fields: **Wireless Management IP**, **Subnet Mask**, **Gateway**, **Wireless Management IP (IPv6)**, **Prefix**, **Gateway (IPv6)IP Interface Name**, and optionally **VLAN ID**.

Note The available fields vary based on the IP address type of the wireless controller. If the wireless controller has only the IPv4 address type, Catalyst Center displays the fields for IPv4 address. If it has only the IPv6 address type, Catalyst Center displays the fields for IPv6 address. If it has both IPv4 and IPv6 address types, Catalyst Center displays the fields for both IPv4 address and IPv6 address.

- For a Mobility Express device, enter values in these fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.
- If you made any changes, click **Save**; otherwise, click **Cancel** to return to the list and configure other devices.

c) From the **Clear Configuration** drop-down list, select any these options:

- **Clear Device Certificates**: Select this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Select this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates**: Select this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Select this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

d) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Apply Image to Other Devices** or **Apply Template to Other Devices**.

You can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

e) If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.

f) After you have configured all the devices, click **Next**.

Step 7 In the **Provision Templates** window, select the template from the **Devices** area, enter your domain name in the **domain** field, and click **Next**.

Step 8 In the **Summary** window, view details about the devices and their configuration preview.

Step 9 Check the **Device Configuration** column for each device to see if the configuration preview succeeded.

If the preview shows an error, you can click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 10 In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

Step 11 Click **Claim**.

Step 12 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

Note If there is a conflicting operation for the selected site, to continue with the current configuration, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see Complete the provisioning process, on page 613.

Provision an AP or sensor device

Use this procedure to claim an AP or sensor device from the Plug and Play Devices list. Alternatively, you can claim a device from the device **Details** window by clicking **Claim**.

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, refer to Plug and Play provisioning prerequisites, on page 588.

Procedure

Step 1 Navigate to the **Plug and Play** to choose the required devices.

a) From the main menu, choose **Provision** > **Plug and Play**.

b) View the devices in the table.

You can use the search bar to find specific devices.

c) Check the check box next to the devices that you want to claim.

d) From the menu bar above the device table, choose **Actions** > **Claim**.

Step 2 (Optional) In the **Assign Site** window, do these steps:

a) Change the device hostname, if needed.

b) Assign a site by doing any of these tasks:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, select a site.
- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Assign this Site to Other Devices**, select the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

If the wireless network profile associated with the assigned site has an onboarding template, Catalyst Center uses this template for PnP onboarding. For more information, refer to Add templates to a network profile, on page 465.

Note In the **System** > **Settings** > **Device Settings** > **PnP AP Location** window:

- If the **Configure AP Location** check box is checked, Configure APs, on page 1382 assigns this site as the AP location during PnP onboarding.
- If the **Configure AP Location** check box is unchecked, Catalyst Center does not configure this site as the AP location during PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow. For more information, refer to Configure APs, on page 1382.

For more information, refer to "Configure AP location for PnP onboarding" in the *Cisco Catalyst Center Administrator Guide*.

c) Click **Next**.

Step 3 In the **Assign Configuration** window, do these steps:

a) In the **Configuration** column, click **Assign** for the device that you want to configure.

b) If the device configuration doesn't need any changes, click **Cancel** and continue to the next step. Otherwise, change or configure any of these settings:

- **Device Name**: Change the device hostname, if needed.
- **Template**: From this drop-down list, select an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

Note If you have not assigned the device to a site, you must choose a template for the device. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

For more information about onboarding APs for non-intent-based network deployments, including Assurance use case and Per-Device Configurations, refer to Onboard APs using PnP for non-intent-based deployments, on page 1448.

- For an AP, select an AP zone from the **AP Zone** drop-down list. The **RF Profile** is auto-populated, and the SSID count appears based on the selected AP zone. When you select the default AP zone, choose the RF profile.
- For an AP, in the **Radio Frequency Profile** drop-down list, select a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.

- For a sensor, in the **Sensor Settings** drop-down list, select the sensor device profile (backhaul) to apply to the device.

  Note For Cisco Aironet 1800s Active Sensor earlier than 1.3.1.2, make sure that you do not select the sensor device profile `CiscoProvisioningSSID`. Instead, select your own SSID for backhaul purposes.

- If you made any changes, click **Save**; otherwise, click **Cancel** to return to the list and configure other devices.

c) From the **Clear Configuration** drop-down list, select any these options:

- **Clear Device Certificates**: Select this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images**: Select this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates**: Select this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels**: Select this option and check the check box next to each of the devices that you want to clear the license level from, and click **Clear**.

d) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and select **Apply Image to Other Devices** or **Apply Template to Other Devices**.

e) If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.

f) After you have configured all the devices, click **Next**.

Step 4 In the **Provision Templates** window, select the template from the **Devices** area, enter your domain name in the **domain** field, and click **Next**.

Note If device is assigned to a site, click **Next**.

Step 5 In the **Summary** window, view details about the devices and their configuration preview.

Step 6 Check the **Device Configuration** column for each device to verify if the configuration preview succeeded.

If the preview shows an error, you can click the **Actions** link in the error message above the table to verify what actions you need to take. You can click an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the device is assigned.

Step 7 In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

Step 8 Click **Claim**.

Step 9 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

Note If there is a conflicting operation for the selected site, to continue with the current configuration, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, refer to Complete the provisioning process, on page 613.

Provision StackWise Virtual Link switch

You can onboard a pair of connected switches as a single logical device with StackWise Virtual Link (SVL) support during PnP onboarding. Currently, SVL PnP onboarding is supported only for Catalyst 9500 Series switches .

Before you begin

- Ensure that both switches are directly connected.
- Connect the switches with links providing a minimum speed of 1 Gbps and ensure that the interface speeds are matched.
- Ensure that the switches are in an initialized state.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 Click **Claim a SVL switch**.

Step 3 In the **Claim as an SVL switch** Pop-up window, provide the values required for the SVL onboarding settings:

a. **Active Switch**: Choose one of the switches as active switch.

b. **Standby Switch**: Choose another switch as the standby switch.

c. **StackWise Virtual Link**: Choose the SVL links. You can choose up to eight SVL links.

d. **Dual-Active Detection Link**: Choose a dual-active detection link if available.

e. **Domain**: Assign a unique value for the domain.

Step 4 Click **Select Site** and choose the desired site for SVL switches.

Step 5 Click **Manage Template** and choose the template to be provisioned to the SVL switches.

Step 6 (Optional) Choose the standard image to be applied after SVL formation.

If the image versions on the devices differ, PnP enforces the selection of a standard image and applies it to both devices before SVL formation.

Step 7 Click **Claim**.

The PnP server creates the SVL and provisions the device.

Complete the provisioning process

During Plug and Play provisioning, only the device credentials and the onboarding configuration are pushed to the device. No other network settings are pushed. After Plug and Play provisioning is completed, you can complete the provisioning process by pushing the network settings that are configured in the **Design** area.

The network settings include AAA server settings, if these are configured. In the case of Cisco ISE, Catalyst Center configures the device on Cisco ISE as a AAA client for RADIUS or TACACS.

Note For Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9000 Series Switches, local AAA configurations are pushed to device when NETCONF is enabled during the day-zero configuration.

For wireless and sensor devices, the network settings include wireless settings, such as RF profiles and antenna radio profiles, if these are configured. For more information, see Wireless device provisioning overview, on page 617.

Before you begin

- Ensure that the device has been provisioned (onboarded) using one of these procedures:
  - Provision a switch or router device, on page 602
  - Provision a wireless controller, on page 606
- Configure network settings. For information, see Configure Network Settings, on page 317.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Select the device and choose **Actions** > **Provision** > **Provision Device**.

Step 3 Proceed through the steps in the workflow.

Step 4 In the **Summary** window, review the remaining network settings. To make any changes, click **Edit** next to the relevant category; otherwise, click **Deploy**.

Note If the device software image version or golden tagged version is 17.14.1 or later, the device claim is blocked if the selected site is configured with MD5 authentication for SNMP credentials.

To claim the device, you must also configure SHA authentication for SNMP credentials, or the software image version must be earlier than 17.14.1. For information on how to configure SHA authentication, see Edit global device credentials, on page 335.

Step 5 (Optional) After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

Delete a device

Deleting a device removes it from the Plug and Play database but does not reset the device. Use **Reset** if you want to reset a device that is in the Error state.

This procedure explains how to delete a device from the Plug and Play Devices list. Alternatively, you can delete a device from the device details window by clicking **Delete**.

Note

- If a device is in the Provisioned state, it can be deleted only from the **Inventory** tab.
- If a device is in a transient state (such as Connecting or Executing), it cannot be deleted from the Plug and Play Devices list.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Check the check box next to one or more devices that you want to delete.

Step 4 From the menu bar above the device table, choose **Actions** > **Delete**.

Step 5 (Optional) For unclaimed devices, check the **Delete Plug and Play capabilities for this device in inventory** check box.

If you choose this option, Catalyst Center deletes the device profile, and the device does not reappear in PnP.

The device remains in inventory and can still be managed. You can re-enable PnP capabilities later.

Step 6 Click **Ok**.

Reset a device

Resetting a device applies only to devices in the Error state and resets its state to Unclaimed and reloads the device, but does not remove it from the Plug and Play database. Use **Delete** if you want to delete a device.

Note If the saved configuration on the device is the factory default or a similar minimal configuration, then this option causes the device to restart the provisioning process. However, if the device has a previously saved startup configuration, then this could prevent the device from restarting the provisioning process and it will need to be reset to factory defaults. On wireless and sensor devices, only the device state is reset and the device is not reloaded.

This procedure shows how to reset a device from the Plug and Play Devices list. Alternatively, you can reset it from the device details window by clicking **Reset**.

Note If a device is in a transient state (such as Connecting or Executing), it cannot be reset.

Procedure

Step 1 From the main menu, choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Check the check box next to one or more devices that you want to reset.

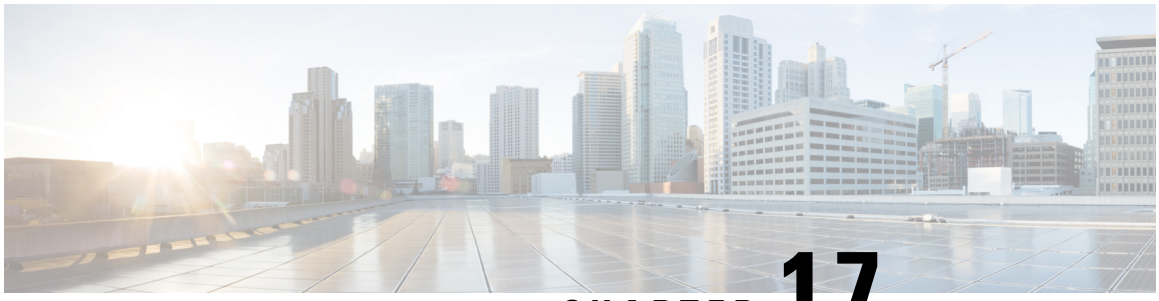
Step 4 Click **Actions > Reset** in the menu bar above the device table.

A confirmation dialog box displays.

Step 5 Choose one of these options:

- **Reset and keep current claim parameters**—Keep the current claim parameters and the device goes to the Planned state.
- **Reset and remove all claim parameters**—Remove the current claim parameters and the device goes to the Unclaimed state.

Step 6 Click **Reset**.



CHAPTER 17

Provision Wireless Devices

- Wireless device provisioning overview, on page 617
- About wireless devices and country codes, on page 617
- Role-based access control, on page 619
- Prerequisites for provisioning a Cisco AireOS Controller, on page 619
- Provision a Cisco AireOS Controller, on page 620
- Provision Cisco APs on day 1, on page 627
- Enable ICMP ping on APs in FlexConnect mode, on page 631
- Day-zero workflow for Cisco AireOS Mobility Express APs, on page 632
- Configure and provision a Cisco Catalyst 9800 Series Wireless Controller, on page 634
- Configure and provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, on page 664
- Renew AP LSC for a wireless device, on page 671
- Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 672
- Inter-Release Controller Mobility introduction, on page 969
- Prerequisites for provisioning a Meraki device, on page 973
- Provision a Meraki device, on page 973
- Provision remote teleworker devices, on page 975

Wireless device provisioning overview

These sections provide information about how to provision various Cisco wireless devices.

About wireless devices and country codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation within that regulatory domain (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Catalyst Center provisions controllers with country codes according to the site they are assigned. In the case of controllers, they can be assigned to more than one site. So, they can be assigned more than one country

code. During provisioning, Catalyst Center assigns sites to the controller along with the sites' country codes. For example, a controller that manages both India and US sites is assigned the IN and US country codes.

When access points are provisioned, they are assigned to a floor. If the access point is a ROW AP, Catalyst Center gets the country code for the site and assigns it to the AP. Any additional APs on the same floor are assigned the same country code.

During AP provisioning with an RF profile selected, out of all the DCA Channels configured on the RF profile, only the supported channels as per the country code are considered for Dynamic Channel Assignment (DCA). You can see the list of unsupported DCA channels in the AP preprovision summary step of the AP provision workflow on Catalyst Center.

The country code information is displayed on the **Device 360** window for controllers and access points.

For a complete list of country codes supported per product, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.

Configure regulatory activation for wireless controllers

Ensure APs associated with a wireless controller obtain a valid country code so their radios become operational.

Regulatory activation is required when APs are unable to obtain a country code through standard geolocation or proximity methods. If a country code is not available, the AP radios are not operational.Catalyst Center uses the regulatory activation file to resolve the country code on these APs.

You can configure regulatory activation for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in nonfabric deployments.

Use this procedure to configure regulatory activation for wireless controllers to resolve the country code on associated APs that have not been able to obtain a country code.

Before you begin

- Obtain the regulatory activation file, in JSON format, from the Meraki dashboard.
- Ensure that the wireless controller is running Cisco IOS XE Release 17.18.1 or later.
- Ensure that the wireless controller is reachable in the inventory.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Select the required wireless controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Regulatory Activation**.

Step 4 In the **Regulatory Activation** slide-in pane, configure the regulatory activation file using one of these options.

If you want to...	Then...
upload a new file	**a.** Use one of these options: • Drag and drop the file into the drag and drop area. • Click **Choose a file**, browse to the location of the file, and click **Open**. **b.** Click **Upload File**.
use an existing file that was uploaded earlier	click **Use existing file**.

Step 5 Under **Uploaded AP Summary**, review the summary of APs and country codes extracted from the uploaded file.

Step 6 Click **Deploy**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Role-based access control

Role-based access control in Catalyst Center allows you to define the capabilities and the permissions that a user has access to. Before provisioning wireless devices, ensure you have access to the sites and devices where you want to provision, along with the necessary permissions to perform provisioning.

For more information, see User profile roles and permissions, on page 23.

Prerequisites for provisioning a Cisco AireOS Controller

- Make sure that you have defined the global network settings before provisioning a Cisco Wireless Controller, including:
  - Network servers, such as AAA, DHCP, and DNS.

    For more information, see Configure global network servers, on page 321.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS.

    For more information, see Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, Add global SNMPv3 credentials, on page 325, and Add global HTTPS credentials, on page 327.
  - IP address pools.

For more information, see Configure IP address pools, on page 337.

- Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles.

Note When you upgrade from an earlier release:

- For WPA3-Enterprise SSIDs, Catalyst Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs.
- For WPA2-WPA3-Enterprise SSIDs, Catalyst Center enables both Dot1x and Dot1x-SHA256 authentication key management settings for the SSIDs.

This configuration might change the intended configuration for the Cisco AireOS Wireless Controllers and wireless controllers running Cisco IOS XE Release 17.6 or earlier. You can update the **Auth Key Management** settings for the SSIDs before reprovisioning the wireless controllers.

For more information, see Configure global wireless settings, on page 350.

- Make sure that you have the wireless controller in your inventory. If not, use the **Discovery** feature to discover the controller.
- Make sure that the wireless controller is added to a site. For more information, see Assign an unprovisioned device to a site, on page 156.
- You cannot reuse any pre-existing VLANs on devices. Provisioning fails if Catalyst Center pushes the same VLAN that already exists on the device.
- You cannot make any configuration changes to the wireless controller that is being managed by the Catalyst Center manually. You must perform all configurations from the Catalyst Center GUI.

Provision a Cisco AireOS Controller

Before you begin

Ensure that the prerequisite is met. For more information, see Prerequisites for provisioning a Cisco AireOS Controller, on page 619.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window display with the discovered devices listed.

Step 2 Expand the **Global** site in the left pane, and select the site, building, or floor that you're interested in.

The available devices in the chosen site display in the **Inventory** window.

Step 3 In the **Devices** table, click the **Search** field. In the **Quick Filters** tab, do these steps:

a) For **Device Family**, click **Wireless Controllers** to get the list of wireless controllers that are discovered.
b) For **Reachability**, click **Reachable** to get the list of wireless controllers that are discovered and reachable.
c) Click **Apply**.

Step 4 Check the check box next to the device name that you want to provision.

Step 5 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays.

Step 6 Click **Choose a site** to assign a site for the wireless controller.

Step 7 In the **Add Sites** window, check the check box next to the site name to associate the wireless controller, and click **Save**.

Step 8 Click **Apply**.

Step 9 Click **Next**.

The **Configuration** window displays.

Step 10 Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.

Step 11 Click **Select Primary Managed AP Locations** to select the managed AP location for the wireless controller.

Step 12 In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, the children under that parent site are automatically selected.

Note Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One wireless controller can manage only one site.

Step 13 Click **Save**.

Step 14 (Optional) Check the **AP Authorization List** check box to choose the authorization list for AP authorization, and do these tasks:

Note This check box is displayed only if an AP authorization list is available. For more information about the AP authorization list, see Create an AP authorization list, on page 417.

- From the **AP Authorization List Name** drop-down list, choose an AP authorization list. Based on the content of the AP authorization list, Catalyst Center displays a message indicating the corresponding primary authorization type and failback mechanism.
- (Optional) To view the entries for the selected AP authorization list, click **View Entries**.
- If the wireless controller manages both mesh and nonmesh APs, Catalyst Center displays the **Authorize Only Mesh Access Points** and **Authorize All Access Points** check boxes.

  To enable authorization for only mesh APs, check the **Authorize Only Mesh Access Points** check box.

  To enable authorization for all APs, check the **Authorize All Access Points** check box.

Step 15 Under **Interface and VLAN Configuration**, click **+ Add** and configure the interface and VLAN details for an active main wireless controller.

Interface and VLAN configuration is applicable for nonfabric wireless controller provisioning only.

The **Configure Interface and VLAN** window displays.

Step 16 From the **Interface Name** drop-down list, choose the interface name.

Note An info icon (ⓘ) is displayed next to the additional interfaces. For more information about additional interfaces, see Configure additional interfaces for a network profile, on page 478.

Step 17 In the **VLAN ID** field, enter a value for the VLAN.

Step 18 In the **Interface IP Address** field, enter a value for the interface IP address.

Step 19 In the **Interface Net Mask (in bits)** field, enter the subnet mask for the interface.

Step 20 In the **Gateway IP Address** field, enter the gateway IP address.

Step 21 From the **LAG/Port Number** drop-down list, choose the link aggregation or the port number.

Step 22 Click **OK**.

Step 23 (Optional) For a guest anchor wireless controller, change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.

Step 24 Click **Next**.

The **Feature Templates** window displays.

Step 25 In the **Devices** pane, you can either search for a feature template by entering its name in the **Find** field, or expand the device and select a feature template.

The selected feature template displays in the right pane.

Step 26 Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the feature template.

You can't edit all the configurations at this step.

Step 27 After making the necessary changes, click **Apply**.

Step 28 Click **Next**.

The **Advanced Configuration** window displays, which is where you can enter the values for predefined template variables.

Step 29 Search for the device or the template in the **Devices** panel.

Step 30 Enter a value for the predefined template variable in the **wlanid** field.

Step 31 Click **Next**.

Step 32 In the **Summary** step, review the device details, and click **Next** to provision the device.

Step 33 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note

- When you provision the wireless controller, Catalyst Center pushes the configuration to the wireless controller and configures it based on the network intent. During the reprovisioning, if there are any out-of-band configurations on the wireless controller that are a part of the network intent or conflicting with the configurations being pushed by Catalyst Center, Catalyst Center overwrites the out-of-band configurations on the wireless controller with the network intent configuration.

  For all the configurations that are supported through the network intent on Catalyst Center, we recommend that you use them instead of out-of-band configurations.

- After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

Step 34 On the **Tasks** window, monitor the task deployment.

Step 35 Provision the secondary controller.

Step 36 The **Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

After provisioning, if you want to make any changes, click **Design**, change the site profile, and provision the wireless controller again.

Step 37 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 38 In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

Step 39 Click **See Details** under **Device Provisioning**.

Step 40 Click **View Details** under **Deployment of network intent**, and click the device name.

Step 41 Expand the **Configuration Summary** area to view the operation details, feature name, and the management capability.

The configuration summary also displays any errors that occurred while provisioning the device.

Step 42 Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.

Configure Cisco Wireless Controller high availability

Cisco Wireless Controller high availability (HA) can be configured through Catalyst Center. Currently, both the formation and breaking of wireless controller HA is supported; switchover options are not supported.

Prerequisites for configuring Cisco Wireless Controller high availability

- The Discovery and Inventory features of wireless controller 1 and wireless controller 2 must be successful. The devices must be managed.
- The service ports and the management ports of wireless controller 1 and wireless controller 2 must be configured.
- The redundancy ports of wireless controller 1 and wireless controller 2 must be physically connected.
- The management address of wireless controller 1 and wireless controller 2 must be in the same subnet. The redundancy management address of wireless controller 1 and wireless controller 2 must also be in the same subnet.

- Manually configure this boot variables on the wireless controller:

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

Configure Cisco Wireless Controller HA

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

Step 2 Check the check box next to the wireless controller name that you want to configure as the primary controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane displays.

Note A warning is displayed at the top of the pane if the wireless controller that you selected isn't assigned to a site. Catalyst Center doesn't push the telemetry configuration to the wireless controller until it's assigned to a site.

By default, the chosen wireless controller becomes the primary controller and the **Primary WLC** field is disabled.

Step 4 Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** address in the respective text boxes.

The IP addresses used for redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the wireless controller. Ensure that these IP addresses are unused IP addresses within that subnet range.

Step 5 From the **Select Secondary WLC** drop-down list, choose the secondary controller.

Note When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated, and an **i** icon displays at the top of the **High Availability** window, along with this message:

Ensure that the Redundancy Management IP and Peer Redundancy Management IP aren’t assigned to any other network entities. If the IPs are in use, change the IP accordingly and configure.

Step 6 Click **Configure HA**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Step 9 When the task is deployed, the HA configuration is initiated in the background using the CLI commands. First, the primary wireless controller is configured. On success, the secondary wireless controller is configured. After the configuration is completed, both wireless controllers reboot. This process may take up to 2.5 minutes to complete.

Step 10 To verify the HA configuration:

a) On the **Provision** > **Inventory** window, click the device that you configured as an HA device.
A dialog box with high-level device information opens.

b) In the dialog box, click **View Details**.

c) Click the **Wireless Info** tab.

The **Redundancy Summary** tab displays the **Sync Status** as **In Progress**. When Catalyst Center finds that HA pairing succeeded, the **Sync Status** changes to **Complete**.

This process is triggered by the inventory poller or manual resynchronization. By now, the secondary wireless controller (wireless controller 2) is deleted from Catalyst Center. This flow indicates a successful HA configuration on the wireless controller.

What happens during or after the high availability process is complete

1. Cisco wireless controller 1 and wireless controller 2 are configured with redundancy management, redundancy units, and SSO. The wireless controllers reboot in order to negotiate their role as active or standby. Configuration is synced from active to standby.
2. On the **Show Redundancy Summary** window, you can see these configurations:
   - SSO is enabled.
   - The wireless controller is active.
   - The wireless controller is in hot standby.
3. The management port of the active wireless controller is shared by both the controllers and will be pointing to the active controller. The user interface, Telnet, and SSH on the standby wireless controller will not work. You can use the console and service port interface to control the standby wireless controller.

Commands to configure and verify high availability

Catalyst Center sends commands to configure Cisco Wireless Controller HA.

Catalyst Center sends the commands to wireless controller 1, including:

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**

- **config redundancy mode sso**

Catalyst Center sends the commands to wireless controller 2, including:

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

Enter these commands to verify the HA configuration from the wireless controller:

- To check HA-related details: **config redundancy mode sso**
- To check the configured interfaces: **show redundancy summary**

Disable high availability configured device in the existing deployment

The Catalyst Center Disable HA feature is supported on Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Wireless Controllers.

Before you begin

Ensure that the HA device in the existing deployment is configured outside of Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

Step 2 Check the check box next to the name of the wireless controller that has the HA feature that you want to disable.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane display.

High Availability slide-in pane shows the **Redundancy Summary** of selected wireless controller configured from outside Catalyst Center.

Step 4 Click **Disable HA**.

Step 5 In the **Warning** dialog box, click **OK**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Step 8 After the task deploys, a success message displays at the bottom of the window indicating that the HA feature has been successfully disabled for the selected wireless controller.

Provision Cisco APs on day 1

Use the procedure to provision APs.

Before you begin

- Make sure that you have Cisco APs in your inventory. If not, use the Discovery feature to discover APs. For more information, see Discover Your Network, on page 55.
- Make sure that you enable the required licenses for the APs on the **License Manager** window. For more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
- If you add new AP zones or SSIDs, you must reprovision the wireless controller. For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.
- If you update the AP zone configurations, you must reprovision the wireless controller. For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.
- If you're using N+1 HA and modify any nonflex SSIDs that are already provisioned on the primary and secondary controllers to flex SSIDs (or conversely), make sure that the states of WLANs are consistent across both the primary and secondary controllers on the corresponding site.

  For example, *SSID1* is configured on a network profile as flex SSID, provisioned on both the primary and secondary controllers, and later modified as nonflex SSID. If you reprovision only the primary controller without reprovisioning the secondary controller, *SSID1* becomes nonflex SSID on the primary controller but remains flex SSID on the secondary controller. If you provision an AP on a site shared by both the primary and secondary controllers, the provisioning fails. To ensure consistency, you must reprovision the secondary controller. When you reprovision the secondary controller, *SSID1* changes to nonflex SSID on the secondary controller too and both controllers have the same state for *SSID1* before provisioning the AP.
- For ROW APs, we recommend that you create an AP profile with the necessary country code and configure custom site tags. For more information, see Configure additional settings for an AP profile for Cisco IOS XE devices, on page 431 and Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

Step 2 Check the check box next to the APs that you want to provision.

You can choose up to 500 APs simultaneously.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 4 If you chose APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue with device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box and choose different APs.

Step 5 In the **Assign Site** step, configure the required parameters.

a) Click **Choose a floor** and assign an AP to the site.

b) In the **Choose a floor** slide-in pane, click the floor where the AP resides and click **Save**.

c) Click **Next**.

Note Catalyst Center doesn't configure this site as the AP location during AP provision. You can configure the AP location using the **Configure Access Points** workflow. For more information, see Configure APs, on page 1382.

Step 6 In the **Configuration** step, configure the required parameters.

a) Click **Advanced Configuration** to configure antenna radio profiles on antenna slots.

Note Advanced configuration is supported on Cisco Catalyst 9130AXE Unified Access Points with Cisco Catalyst 9800 Series Wireless Controller software release 17.6 or later. Global tri-radio mode is enabled on the wireless controller and configured during AP provisioning.

For information about antenna radio profile, see Create an antenna radio profile, on page 440.

b) Configure the beam selection value for AP radio slots from the **Slot 1** and **Slot 2** drop-down lists.

c) Click **Save**.

d) From the **AP Zone Name** drop-down list, choose an AP zone.

Note This drop-down list is enabled only when AP zones are added to the network profile for the site.

If you choose an AP zone, the RF profile is inherited from the AP zone configuration.

e) From the **RF Profile** drop-down list, use the default settings or choose a different value from the list.

The default RF profile is the custom profile that you marked as default under the **Design** > **Network Settings** > **Wireless** > **RF Profiles** > **Basic RF Profile** tab.

Note This drop-down list is disabled if you choose an AP zone from the **AP Zone** drop-down list.

f) In the **Mesh Role** drop-down list, choose **Root** or **Mesh**.

For information about wireless mesh networks, see About wireless mesh networks, on page 449.

g) Click **Next**.

Step 7 In the **Summary** step, review the device details, and click **Next** to provision the AP.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Step 10 You're prompted with a message that the creation or modification of an AP group is in progress and then a message that APs will reboot after provisioning. Click **OK**.

The **Last Sync Status** column in the **Inventory** window shows `SUCCESS` for a successful deployment.

Migrate APs from a Wireless Controller to another Wireless Controller

Use this procedure to migrate APs from one wireless controller to another wireless controller with the same floors in the network hierarchy.

Before you begin

- Ensure that the old wireless controller (for example, *WC1*) is provisioned with the required sites (for example, *Building-1* with *Floor-1*, *Floor-2*, and *Floor-3)* as the primary-managed AP location.
- Ensure that the APs that need to be migrated are provisioned on the floors managed by the old wireless controller (for example, *Building-1*/*Floor-1*, *Building-1*/*Floor-2*, *Building-1*/*Floor-3* managed by *WC1*).

Procedure

Step 1 Add a new building and floor to the network hierarchy (for example, *Building-New* with *Floor-New*). For more information, see Add, edit, and delete a building, on page 242 and Add, edit, and delete a floor, on page 242.

Step 2 Create a wireless network profile and assign it to the newly added floor (*Floor-New*). For more information, see Create network profiles for wireless, on page 460.

Step 3 Reprovision the old wireless controller with the newly added floor (*Floor-New*) as the primary-managed AP location and remove the old sites (*Floor-1*, *Floor-2*, and *Floor-3*). For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 4 Provision the new wireless controller (for example, *WC2*) with the old sites (*Floor-1*, *Floor-2*, and *Floor-3*) as the primary-managed AP locations. For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 5 Use the **Configure Access Points** workflow to change the primary wireless controller name and IP address. In the **Configure AP Parameters** window of this workflow, do these steps:

a) Check the **High Availability** check box.
b) From the **Select Primary Controller Name** drop-down list, choose the new wireless controller (*WC2*).
c) In the **Primary Controller IP Address** field, enter the IP address of the new wireless controller (IP address of *WC2*).

For more information, see Configure APs, on page 1382.

Step 6 Do these steps to ensure that the APs have joined the new wireless controller (*WC2*):

a) From the main menu, choose **Provision** > **Inventory**.
b) Click the **Access Points** device family button at the top of the **Inventory** window.
c) Hover your cursor over the **Focus** drop-down list, and choose **Inventory**.
d) Under the **Associated WLC IP** column, check the IP address of the corresponding wireless controller for the APs.

If this column isn't displayed, click the gear icon at the top-right corner of the window and customize the table settings to display the column. For more information, see Display information about your inventory, on page 80.

Note If the AP is flapping and assigned with the AUTO_INV_EVENT_SYNC_DISABLED or INV_EVENT_SYNC_DISABLED tag, automatic synchronization of events on the AP is disabled. After the underlying cause of the AP flapping is resolved, we recommend that you perform a manual synchronization to display the most current AP details. Alternatively, wait for the next scheduled synchronization to update the AP information.

Step 7 Reprovision the APs to deploy the latest configuration. For more information, see Provision Cisco APs on day 1, on page 627.

Reset APs

Using the Factory Reset feature, you can clear the configurations on the APs and reset them to the default configuration. After the AP configurations are cleared, the APs reboot.

Important Resetting an AP disrupts the network connectivity for all the associated clients.

Before you begin

Ensure that the APs are reachable.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.
The **Inventory** window displays the list of discovered devices.

Step 2 In the **Devices** table, click the **Access Points** device family button to display the list of available APs.

Step 3 Check the check box next to the APs that you want to reset.

You can select up to 100 APs for factory reset.

Step 4 From the **Actions** drop-down list, choose **Provision** > **Factory Reset**.
The **Factory Reset** slide-in pane opens.

Step 5 Under **Factory Reset**, choose one of these options:

- **Clear all configuration**: Clears all the configurations on the AP and resets it to the default configuration.
- **Clear all configuration except static IP**: Clears all the configurations on the AP, except the static IP configuration.

Step 6 Under **Schedule Task**, do these steps:

a) Choose one of these options:

- **Now**: Immediately reset the APs.
- **Later**: Schedule the AP reset for a later date or time.

b) (Optional) In the **Task Name** field, update the task name.

c) If you chose **Later**, do these tasks:

- Under **Start Date/Time**, specify a start date and time for the task.
- From the **Time Zone** drop-down list, choose a time zone for the task.

Step 7 To view the APs selected for reset, expand the **Selected Devices** drop-down list.

Step 8 Click **Apply**.

To view the status of AP reset, go to the **Activities** > **Tasks** window and open the relevant work item.

Enable ICMP ping on APs in FlexConnect mode

You can enable Internet Control Message Protocol (ICMP) ping on APs that are in FlexConnect mode and in an unreachable state. Catalyst Center uses the ICMP to ping FlexConnect APs that are in unreachable state every 5 minutes to enhance reachability and then updates the reachability status in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Device Settings** > **ICMP Ping**.

Step 2 Check the **Enable ICMP ping for unreachable access points in FlexConnect mode** check box to enable the ICMP ping.

Step 3 Click **Save**.

This success message displays: `ICMP Ping status updated successfully`.

Catalyst Center starts pinging FlexConnect APs that are disassociated from Cisco Wireless Controllers but are reachable. You can view the reachability status in the **Inventory** window.

Step 4 To view the reachability status, choose **Provision** > **Inventory**.

Step 5 The **Reachability** column shows **Ping Reachable** when the device is reachable by the ICMP ping.

Day-zero workflow for Cisco AireOS Mobility Express APs

Before you begin

The Cisco Mobility Express wireless network solution comprises at least one 802.11ac Wave 2 Cisco Aironet Series access point with an in-built, software-based wireless controller managing other APs in the network. The AP acting as the wireless controller is referred to as the *primary AP*. The other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as *subordinate APs*.

- Design your network hierarchy with sites, buildings, floors, and so on. For more information, see Create, edit, and delete a site, on page 240, Add, edit, and delete a building, on page 242, and Add, edit, and delete a floor, on page 242.
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites. For more information, see Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, and Add global SNMPv3 credentials, on page 325.
- Create WLANs, interfaces, and RF profiles.
- Configure the DHCP server with Option #43 or Option #60. This is the IP address of the Catalyst Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- Make sure that you have Mobility Express APs in the inventory. If not, discover them using the Discovery feature. For more information, see Discover your network using CDP, on page 66, Discover your network using an IP address range or CIDR, on page 68, and About Inventory, on page 78.
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

Procedure

Step 1 The Cisco Mobility Express contacts the DHCP server and connects to the Catalyst Center Plug and Play server.

Step 2 The DHCP server allocates the IP address with Option #43, which is the IP address of the Catalyst Center Plug and Play server.

Step 3 The Mobility Express AP starts the PnP agent and contacts the PnP server.

Note If you have a set of Mobility Express APs in the network, they go through an internal protocol. The protocol selects one Mobility Express AP, which will be configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

Step 4 Find the unclaimed AP in the **Provision** > **Network Devices** > **Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the **Onboarding Status** to become **Initialized**.

Step 5 To claim the AP, check the check box next to the AP device name.

Step 6 Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window displays.

Step 7 In the **Site Assignment** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

Step 8 Click **Next**.

Step 9 To configure a device, click the device name in the **Configuration** window.

Step 10 In the **Configuration for device name** window, assign the static IP details for the device:

- **Management IP**
- **Subnet Mask**
- **Gateway**

Step 11 Click **Save**.

Step 12 Click **Next**.

The **Summary** window is displayed.

Step 13 Click **Claim** in the **Summary** window.

After the Mobility Express AP is claimed, the configured IP address is assigned to the Mobility Express AP.

The claimed device, which is an AP, and the wireless controller are now available under **Provision** > **Device Inventory** > **Inventory**.

Step 14 (Optional) Add devices in bulk from a CSV file.

For more information, see Add devices in bulk, on page 597.

When you bulk import Mobility Express APs through a CSV file, all the Mobility Express APs appear on the **Devices** > **Plug and Play** window. Based on the VRRP protocol, only one Mobility Express AP among the imported ME APs becomes the primary AP. The remaining APs become subordinate APs. After claiming the primary AP, you don't need to claim the subordinate APs. Catalyst Center does not clear the subordinate APs from the **Plug and Play** window. You must delete those subordinate APs manually from the **Devices** > **Plug and Play** window.

Step 15 To provision the Cisco Wireless Controller, see Provision a Cisco AireOS Controller, on page 620.

Configure and provision a Cisco Catalyst 9800 Series Wireless Controller

Cisco Catalyst 9800 Series Wireless Controller overview

The Cisco Catalyst 9800 Series Wireless Controller is the next generation of wireless controllers built for intent-based networking. The Cisco Catalyst 9800 Series Wireless Controller is Cisco IOS XE based and integrates the RF excellence from Aironet with the intent-based networking capabilities of Cisco IOS XE to create the best-in-class wireless experience for your organization.

The Cisco Catalyst 9800 Series Wireless Controller is built on a modular operating system and uses open, programmable APIs that enable automation of day-zero and day-*n* network operations.

The Cisco Catalyst 9800 Series Wireless Controller is available in multiple form factors:

- Catalyst 9800-40 Wireless Controller.
- Catalyst 9800-80 Wireless Controller.
- Catalyst 9800-CL Cloud Wireless Controller: Deployable on private cloud (ESXi, KVM, Cisco ENCS, and Hyper-V) and manageable by Catalyst Center.
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, Catalyst 9400 Series Switches, and Catalyst 9500H Series Switches.
- Cisco Catalyst 9800-L Wireless Controller: Provides seamless software updates for small- to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.

This table lists the supported virtual and hardware platforms for the Cisco Catalyst 9800 Series Wireless Controller:

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	Supports up to 6000 access points and 64,000 clients. Supports up to 80 Gbps throughput and occupies a 2-rack unit space. Modular wireless controller with up to 100-GE uplinks and seamless software updates.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-sized organizations and campus deployments. Supports up to 2000 access points and 32,000 clients. Supports up to 40 Gbps throughput and occupies a 1-rack unit space. Provides four 1-GE or 10-GE uplink ports.

Platform	Description
Cisco Catalyst 9800-CL Cloud Wireless Controller	Cisco Catalyst 9800-CL Cloud Wireless Controller can be deployed in a private cloud or a public cloud as Infrastructure as a Service (IaaS). Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security. A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller for private cloud supports ESXi, KVM, Cisco ENCS, and Hyper-V hypervisors.
Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches	Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches bring the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Cisco SD-Access, which is a highly secure solution for small campuses and distributed branches. The embedded controller supports access points (APs) only in Fabric mode.
Cisco Catalyst 9800-L Wireless Controller	Cisco Catalyst 9800-L Wireless Controller provides seamless software updates for small to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network. • Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45) • Cisco Catalyst 9800-L Fiber Series Wireless Controller 9800-L-F SFP)

This table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[3] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 • Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 and 3.9.1

[3] Installing the .ova file of C9800-CL using ESXi vSphere does not work. This is not limited to the C9800 ova but affects other products. Cisco and VMware are actively working to fix the issue. Contact your Cisco account representative to see if the problem is fixed. There are issues specific to VMware 6.5 and C9800-CL OVA file deployment in which deployment fails with the warning "A required disk image was missing" and the error "Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files." To install C9800-CL on VMware ESXi 6.5, do one of these tasks: 1) Install the .iso file of C9800-CL using the ESXi embedded GUI (ESXI 6.5 client version 1.29.0 is tested and required). 2) Install the .ova file of C9800-CL using the OVF tool.

This table lists the Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) versions supported in Catalyst Center:

Note Cisco Enterprise NFVIS devices support the N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 3.12.x only is supported. Upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 4.1.x is not supported.

Cisco Enterprise NFVIS version	Enterprise network compute system device platform	Notes
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Catalyst Center supports these NFVIS upgrade paths: NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2. Cisco Enterprise NFVIS 3.12.1 is not supported on any versions of Catalyst Center. Upgrade to Cisco Enterprise NFVIS 3.12.1 from Cisco Enterprise NFVIS 3.11.x using Catalyst Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from Cisco Enterprise NFVIS 3.12.1 using Catalyst Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from 3.11.2 is supported using Catalyst Center. Cisco Enterprise NFVIS 3.12.2 is supported on Catalyst Center.
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS does not support Cisco Enterprise NFVIS 3.10.x.

Configure a Cisco Catalyst 9800 Series Wireless Controller in Catalyst Center

1. Install Catalyst Center.

   For more information, see the Cisco Catalyst Center Installation Guide.

2. For information on software image upgrade, see Software image upgrade support for Cisco Catalyst 9800 Series Wireless Controller, on page 640.

3. Log in to the Catalyst Center GUI and verify that the applications you need are in the **Running** state.

   From the main menu, choose **System Settings** > **Software Updates** > **Installed Apps**.

4. Integrate Cisco Identity Services Engine with Catalyst Center. After integration, any devices that Catalyst Center discovers along with relevant configurations and data are pushed to Cisco ISE.

5. Discover the Cisco Catalyst 9800 Series Wireless Controller.

   You must enable NETCONF and set the port to 830 to discover the Cisco Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

For more information, see Discover your network using CDP, on page 66 or Discover your network using an IP address range or CIDR, on page 68.

You must add the wireless management IP address manually.

Note On the Cisco Catalyst 9800 Series Wireless Controller, you must configure a static IP address for the wireless management interface to prevent provisioning failure.

While performing discovery using the Cisco Discovery Protocol (CDP) or an IP address range in the **Discovery** window, choose **Use Loopback** from the **Preferred Management IP** drop-down list to specify the device's loopback interface IP address.

6. Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.

   For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.

   You must wait for the devices to move to a **Managed** state.

7. To verify the Assurance connection with the Cisco Catalyst 9800 Series Wireless Controller, use these commands:

   - **#show crypto pki trustpoints | sec DNAC-CA**

     ```
     Trustpoint DNAC-CA
         Subject Name:
         cn=kube-ca
               Serial Number (hex): 00E***************
         Certificate configured.
     ```

   - **#show crypto pki trustpoints | sec sdn-network**

     ```
     Trustpoint sdn-network-infra-iwan:
         Subject Name:
         cn=sdn-network-infra-ca
             Serial Number (hex): 378***************
         Certificate configured.
     ```

   - **#show telemetry ietf subscription all**

     ```
     Telemetry subscription brief

       ID               Type        State       Filter type
       -----------------------------------------------------
       1011             Configured  Valid       tdl-uri
       1012             Configured  Valid       tdl-uri
       1013             Configured  Valid       tdl-uri
     ```

   - **#show telemetry internal connection**

     ```
     Telemetry connection

     Address Port Transport State Profile
     ------------------------------------------------------------
     IP address 25103 tls-native Active sdn-network-infra-iwan
     ```

   - **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. Configure a TACACS server while configuring authentication and policy servers.

   Configuring TACACS is not mandatory if you have configured the username locally on the Cisco Catalyst 9800 Series Wireless Controller.

9. Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

   You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Catalyst Center.

   To import and upload an existing network hierarchy, see Import your site hierarchy to Catalyst Center, on page 233.

   To create a new network hierarchy, see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

10. Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

    For more information, see Work with APs on a floor map, on page 256.

11. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

    For more information, see Network settings overview, on page 317, Configure global network servers, on page 321, and Add AAA server.

12. Create a wireless radio frequency profile with the parent profile as custom.

    For more information, see Create a wireless radio frequency profile, on page 383.

13. Create IP address pools at the global level.

    Catalyst Center uses IP address pools to automate the configuration and deployment of SD-Access networks.

    To create an IP address pool, see Configure IP address pools, on page 337.

    You must reserve an IP address pool for the building that you are provisioning. For more information, see Reserve IP Address Pools.

14. Create enterprise and guest wireless networks. Define the global wireless settings once; Catalyst Center then pushes the configurations to various devices across geographical locations.

    Designing a wireless network is a two-step process. First, you must create SSIDs, and then associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

Note When you upgrade from an earlier release:

- For WPA3-Enterprise SSIDs, Catalyst Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs.
- For WPA2-WPA3-Enterprise SSIDs, Catalyst Center enables both Dot1x and Dot1x-SHA256 authentication key management settings for the SSIDs.

This configuration might change the intended configuration for the Cisco AireOS Wireless Controllers and wireless controllers running Cisco IOS XE Release 17.6 or earlier. You can update the **Auth Key Management** settings for the SSIDs before reprovisioning the wireless controllers.

For more information, see Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366. For information about other wireless settings, see Configure global wireless settings, on page 350.

15. Configure the backhaul settings. For more information, see Manage backhaul settings, on page 439.
16. In the **Policy** window for the Cisco Catalyst 9800 Series Wireless Controller, do this configuration:
    - Create a virtual network. The virtual network segments your physical network into multiple logical networks.
    - Create a group-based access control policy and add a contract. For more information, see Create group-based access control policy, on page 1192.
17. Configure high availability.

    For more information, see Configure high availability for the Cisco Catalyst 9800 Series Wireless Controller, on page 641.
18. Provision the Cisco Catalyst 9800 Series Wireless Controller with the configurations added during the design phase.

    For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.
19. Configure and deploy application policies on the Cisco Catalyst 9800 Series Wireless Controller.

    For more information, see Create an application policy, on page 1231, Deploy an application policy, on page 1237, and Edit an application policy, on page 1235.

Note You must provision Cisco Catalyst 9800 Series Wireless Controller devices before deploying an application policy.

For Cisco Catalyst 9800 Series Wireless Controller devices, two different policies with different business relevance for two different SSIDs do not work. The last deployed policy always takes precedence when you are setting up relevance.

For Cisco Catalyst 9800 Series Wireless Controller devices, changing the default business relevance for an application does not work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

Software image upgrade support for Cisco Catalyst 9800 Series Wireless Controller

Before you begin

- Discover the Cisco Catalyst 9800 Series Wireless Controller.

  Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller. NETCONF enables wireless services on the controller and provides a mechanism to install, manipulate, and delete the configuration of network devices.

  For more information, see Discover your network using CDP, on page 66, or Discover your network using an IP address range or CIDR, on page 68.

- Make sure that the devices appear in the device inventory and are in the **Managed** state.

  For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.

Procedure

Step 1 From the main menu, choose **Design** > **Image Repository**.

The **Inventory** window displays with the discovered devices listed.

Step 2 Import the Cisco Catalyst 9800 Series Wireless Controller software image from your local computer or from a URL.

For more information, see Import a software image, on page 539.

Step 3 Assign the software image to a device family.

For more information, see Manage software image assignment for a device family, on page 540.

Step 4 You can mark a software image as Golden by clicking the star for a device family or a particular device role.

For more information, see Mark a software image as standard, on page 545.

Step 5 Provision the software image.

From the main menu, choose **Provision** > **Device** > **Inventory**.

Step 6 In the **Inventory** window, check the check box next to the Cisco Catalyst 9800 Series Wireless Controller whose image you want to upgrade.

Step 7 From the **Actions** drop-down list, choose **Software Image** > **Image Update**.

For more information, see Provision a software image, on page 551.

Configure high availability for the Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Configuring high availability (HA) on the Cisco Catalyst 9800 Series Wireless Controller involves these prerequisites:

- Both the Cisco Catalyst 9800 Series Wireless Controllers are running the same software version and have the active software image on the primary wireless controller.
- The service ports and management ports of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured.
- The redundancy ports of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are physically connected.
- Preconfigurations such as interface configurations, route addition, ssh line configurations, and NETCONF-YANG configurations are completed on the Catalyst 9800 Series Wireless Controller appliance.
- The management interface of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are in the same subnet.
- The discovery and inventory of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 devices are successful from Catalyst Center.
- The devices are reachable and in the **Managed** state.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

Step 2 To view devices available in a particular site, expand the **Global** site in the left pane, and choose the site, building, or floor that you're interested in.

All the devices available in that chosen site display in the **Inventory** window.

Step 3 In the **Devices** table, click the **Search** field. In the **Quick Filters** tab, do these steps:

a. For **Device Family**, click **Wireless Controllers** to get the list of wireless controllers that are discovered.

b. For **Reachability**, click **Reachable** to get the list of wireless controllers that are discovered and reachable.

c. Click **Apply**.

Step 4 In the **Inventory** window, check the check box next to the required Cisco Catalyst 9800 Series Wireless Controller name to configure it as a primary controller.

Step 5 Hover your cursor over **Actions** and choose **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane displays.

Note A warning displays at the top of the pane if the selected controller isn't assigned to a site. Catalyst Center doesn't push its telemetry configuration to the controller until it's assigned to a site.

By default, the selected Catalyst 9800 Series Wireless Controller becomes the primary controller and the **Primary C9800** field is disabled.

Step 6 For Cisco Catalyst 9800-CL Wireless Controllers, from the **Select Primary Interface** and **Select Secondary Interface** drop-down lists, choose the interface that is used for HA connectivity.

The HA interface serves these purposes:

- Enables communication between the controller pair before the IOSd boots up.
- Provides transport for IPC across the controller pair.
- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

Step 7 From the **Select Secondary C9800** drop-down list, choose the secondary controller to create an HA pair.

Note When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated, and an **i** icon displays at the top of the **High Availability** window, along with this message:

Ensure that the Redundancy Management IP and Peer Redundancy Management IP aren’t assigned to any other network entities. If the IPs are in use, change the IPs accordingly and configure.

Step 8 Enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses in the respective fields.

Note
- The IP addresses used for the redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the Cisco Catalyst 9800 Series Wireless Controller. Ensure that these IP addresses are unused IP addresses within the subnet range.
- Catalyst Center only pushes the management IP address of the Cisco Catalyst 9800 Series Wireless Controller to the Cisco ISE network access device list. Whereas the standby controller uses the redundancy management IP address to initiate AAA requests. So, you must add the redundancy management IP addresses to the AAA servers for a seamless client authentication and standby monitoring.

Step 9 From the **Netmask** drop-down list, choose the netmask address.

Step 10 Click **Configure HA**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note The **Preview Configuration** window displays the configurations for the primary wireless controller and secondary wireless controller.

Step 12 On the **Tasks** window, monitor the task deployment.

When the task is deployed, the HA configuration is initiated in the background using the CLI commands. First, the primary controller is configured. On success, the secondary controller is configured. Both the devices reboot once the HA is enabled. This process may take up to 2.5 minutes to complete.

Step 13 To verify the HA configuration:

a) On the **Provision** > **Inventory** window, click the device that you configured as an HA device.
A dialog box with high-level device information opens.

b) In the dialog box, click **View Details**.

c) Click the **Wireless Info** tab.

The **Redundancy Summary** tab displays the **Sync Status** as **HA Pairing is in Progress**. When Catalyst Center finds that the HA pairing is successful, the **Sync Status** becomes **Complete**.

This process is triggered by the inventory poller or manual resynchronization. By now, the secondary controller (Catalyst 9800 Series Wireless Controller 2) is deleted from Catalyst Center. This flow indicates successful HA configuration in the Catalyst 9800 Series Wireless Controller.

Step 14 To manually resynchronize the controller:

a) On the **Provision** > **Inventory** window, check the check box next to the controller that you want to synchronize manually.

b) From the **Actions** drop-down list, choose **Inventory** > **Resync Device**.

What to do next

These actions occur after the HA process completes:

- Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured with redundancy management, redundancy units, and Single sign-on (SSO). The devices reboot to negotiate their role as an active controller or a standby controller. The configuration is synchronized from active to standby.

Note If you've configured a AAA server or Cisco ISE server for client and endpoint authentication in Catalyst Center then in a HA setup, the CTS credentials for active and standby controllers are synchronized and hence, during a HA switchover, Catalyst Center doesn't update the CTS credentials for the wireless controllers on Cisco ISE.

- On the **Show Redundancy Summary** window, you can see these configurations:

- SSO is enabled.
- The Catalyst 9800 Series Wireless Controller 1 is in the active state.
- The Catalyst 9800 Series Wireless Controller 2 is in the standby state.

Information about high availability

High availability (HA) allows you to reduce the downtime of wireless networks that occurs because of the failover of controllers. You can configure HA on Cisco Catalyst 9800 Series Wireless Controller through Catalyst Center.

Commands to configure high availability on Cisco Catalyst 9800 Series Wireless Controllers

Procedure

Step 1 Use these commands to configure HA on the primary controller for Cisco Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 192.0.2.2 255.255.255.0
  remote-ip 192.0.2.3
  ```

- Run the **reload** command to reload devices for the changes to become effective.

Step 2 Use these commands to configure HA on the secondary controller for Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

  ```
  chassis ha-interface GigabitEthernet 2 local-ip 192.0.2.3 255.255.255.0
  remote-ip 192.0.2.2
  ```

Step 3 Run the **chassis clear** command to clear or delete all the HA-related parameters, such as the local IP, remote IP, HA interface, mask, timeout, and priority.

Note Reload the devices for changes to take effect by running the **reload** command.

Step 4 Use these commands to configure HA on the primary controller for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

```
chassis ha-interface local-ip 192.0.2.2 255.255.255.0 remote-ip 192.0.2.3
```

- Run the **reload** command to reload devices for the changes to become effective.

Step 5 Use these commands to configure HA on the secondary controller for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure an HA chassis interface:

```
chassis ha-interface local-ip 192.0.2.3 255.255.255.0 remote-ip 192.0.2.2
```

Step 6 Run the **chassis clear** command to clear or delete all the HA-related parameters, such as the local IP, remote IP, HA interface, mask, timeout, and priority.

Note Reload the devices for changes to take effect by running the **reload** command.

Commands to verify Cisco Catalyst 9800 Series Wireless Controllers high availability

Use these commands to verify the high availability configurations from Cisco Catalyst 9800 Series Wireless Controller:

- Run the **config redundancy mode sso** command to check the HA-related details.
- Run the **show chassis** command to view chassis configurations about the HA pair, including the MAC address, role, switch priority, and current state of each controller device in the redundant HA pair.
- Run the **show ip interface brief** command to view the actual operating redundancy mode running on the device, and not the configured mode as set by the platform.
- Run the **show redundancy states** command to view the redundancy states of the active and standby controllers.
- Run the **show redundancy summary** command to check the configured interfaces.
- Run the **show romvar** command to verify high availability configuration details.

N+1 high availability

Overview of N+1 high availability

Catalyst Center supports N+1 high availability (HA) on Cisco AireOS wireless controllers and Cisco Catalyst 9800 Series Wireless Controllers.

Cisco AireOS wireless controllers have a dedicated stock-keeping unit (SKU) for their N+1 controllers. Cisco Catalyst 9800 Series Wireless Controllers don't have a dedicated SKU; the same model and same PID must be used for HA. For example, a Cisco Catalyst 9800-80 must be paired with another 9800-80.

The N+1 HA architecture provides redundancy for controllers across geographically separated data centers with low-cost deployments.

N+1 HA allows Cisco Wireless Controllers to be used as backup controllers for multiple primary controllers. These wireless controllers are independent of each other and do not share configuration or IP addresses on any of their interfaces. When a primary wireless controller resumes operation, the APs fall back automatically from the backup wireless controller to the primary wireless controller if the AP fallback option is enabled.

Catalyst Center supports primary and secondary controller configurations for N+1 HA.

N+1 HA is configured at the AP level, not at the global level. Configurations are pushed directly to the AP.

APs with higher priority on the primary controller always connect first to the backup controller, even if they have to push out the lower priority APs.

The N+1 HA configuration has these limitations:

- Auto provisioning of a secondary controller is not supported because of the VLAN ID configuration.
- You must reprovision the secondary controller manually with the latest design configuration if you made any changes to the primary controller.
- Catalyst Center does not support fault tolerance.
- Access Point Stateful Switch Over (AP SSO) functionality is not supported for N+1 HA. The AP Control and Provisioning of Wireless Access Points (CAPWAP) state machine is restarted when the primary controller fails.

Prerequisites for configuring N+1 high availability from Catalyst Center

- Discover primary and the secondary controller by running the Discovery feature.

  For more information, see Discover your network using CDP, on page 66, or Discover your network using an IP address range or CIDR, on page 68.

- Make sure that the wireless controllers are reachable and in the Managed state.

  For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.

- Verify the network connectivity between devices. If the primary controller goes down, the AP should be able to join the secondary controller through the N+1 configuration.

- Create two buildings to manage the primary and secondary locations for both devices. For example, create two buildings, *Building A* and *Building B*, where Building A is the primary managed location for controller-1 and also the secondary managed location for controller-2, and Building B is configured only as a primary managed location for controller-2.

  For more information, see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

- Add and position APs on a floor map to get a coverage heatmap visualization during the design phase.

  For more information, see Work with APs on a floor map, on page 256.

- Create two SSIDs and associate them as the backhaul SSIDs.

  For more information, see Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

Configure N+1 high availability from Catalyst Center

This procedure shows how to configure N+1 high availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

Step 2 Check the check box next to the desired controller to provision it as a primary controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays.

Step 4 Click **Choose a site** to assign a primary-managed AP location for the primary controller.

Step 5 In the **Choose a site** window, select a site and click **Save**.

Step 6 Click **Next**.

The **Configuration** window displays, which shows the primary-managed AP location for the primary device.

Step 7 Add or update the managed AP locations for the primary controller by clicking **Select Primary Managed AP Locations**.

Step 8 In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.

You can either select a parent site or the individual sites.

Step 9 Configure the interface and VLAN details.

Step 10 Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details, and click **Next**.

Step 11 In the **Advanced Configuration** window, configure the values for the predefined template variables, and click **Next**.

Step 12 In the **Summary** window, verify the managed AP locations for the primary controller and other configuration details, and click **Next**.

Step 13 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 14 On the **Tasks** window, monitor the task deployment.

Step 15 To provision the secondary controller, in the **Inventory** window, check the check box next to the desired controller to provision it as a secondary controller.

Step 16 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays.

Step 17 Click **Choose a site** to assign the managed AP location for the secondary controller.

The managed AP location for the secondary controller should be the same as the managed AP location of the primary controller.

Step 18 In the **Choose a site** window, check the check box next to the site name to associate the secondary controller, and click **Save**.

Step 19 Click **Next**.

The **Configuration** window displays, which shows the primary AP managed and secondary-managed AP locations for the secondary device.

Step 20 Add or update the managed AP locations for the secondary controller by clicking **Select Secondary Managed AP Locations**.

Step 21 In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.

You can either select a parent site or the individual sites.

Step 22 Configure the interface and VLAN details for the secondary controller.

Step 23 Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details for the secondary controller, and click **Next**.

Step 24 In the **Advanced Configuration** window, configure the values for the predefined template variables, and click **Next**.

Step 25 In the **Summary** window, verify the managed AP locations for the secondary controller and other configuration details, and click **Next**.

Step 26 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 27 On the **Tasks** window, monitor the task deployment.

Step 28 To verify the managed locations of the primary and secondary controllers, click the device name of the controllers that you provisioned on the **Provision** > **Inventory** window.

Step 29 In the dialog box, click **View Device Details**.

Step 30 In the device details window, click the **Wireless Info** tab to view the primary and secondary managed location details.

Step 31 Provision the AP for the primary controller. For more information, see Provision Cisco APs on day 1, on page 627.

Mobility configuration overview

The mobility configuration in Catalyst Center allows you to group a set of Cisco Wireless Controllers into a mobility group for a seamless roaming experience of wireless clients.

By creating a mobility group, you can enable multiple wireless controllers in a network to dynamically share information and forward traffic when inter-controller or inter-subnet roaming occurs. Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different wireless controllers within the same wireless network.

Catalyst Center allows you to create mobility groups between various platforms, such as Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

The mobility configuration has these guidelines and limitations:

- You cannot select multiple controllers for configuring mobility on the **Provision** window.
- You cannot create mobility groups with the group name as default. This resets the mobility and RF group names as default and deletes all the peers.
- You cannot configure a mobility group name on the anchor controller.
- You must reboot the wireless controller manually if there is a change to the virtual IP address when configuring mobility groups on Cisco AireOS Controllers.
- Wireless controllers with the same mobility group name are automatically grouped into a single mobility group and added as peers to each other.
- When configuring mobility groups on Cisco AireOS Controllers, if the wireless controllers do not have the IP address 192.0.2.1, Catalyst Center pushes the virtual IP address 192.0.2.1 to all the wireless controllers.
- Do not explicitly add guest anchor controllers to the mobility group. The provisioned guest anchor controllers do not appear in the drop-down list while adding peers in the mobility configuration window.
- If you provision a wireless controller as a guest anchor, ensure that it is not added to the mobility group.

Mobility configuration workflow

Here is the workflow that you can follow to configure mobility on Cisco Wireless Controller:

- To configure mobility, you must provision a wireless controller with the mobility group name, RF group name, and mobility peers.
- The configuration that is applied during the wireless controller provisioning is automatically replicated to all the mobility peers configured in that group.
- Resynchronize the wireless controllers to get the latest tunnel status.

Mobility configuration use cases

These use cases explain the steps to configure mobility between controllers.

Use case 1

This use case assumes that wireless controller 1, wireless controller 2, and wireless controller 3 are newly added to Catalyst Center with the mobility group name, "Default." These wireless controllers aren't yet provisioned.

1. Provision wireless controller 1 by configuring the mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. Provision wireless controller 2.

   In the **Provision** window, the mobility configuration is automatically populated for wireless controller 2 with the group name and peers.
3. Provision wireless controller 3.

4. After provisioning all the wireless controllers, resynchronize the wireless controllers to receive the latest tunnel status.

Use case 2

This use case assumes that wireless controller 1, wireless controller 2, and wireless controller 3 have already been added to Catalyst Center with different mobility group names. These wireless controllers are provisioned.

1. Provision wireless controller 1 by configuring the mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. The mobility configuration is automatically replicated across other peers, such as wireless controller 2 and wireless controller 3.
   - After the successful provisioning of wireless controller 1, wireless controller 2 and wireless controller 3 are added as peers on the wireless controller 1.
   - On wireless controller 2, wireless controller 1 and wireless controller 3 are added as peers.
   - On wireless controller 3, wireless controller 1 and wireless controller 2 are added as peers.

Configure mobility group

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays, which lists all the discovered devices.

Step 2 Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller name for which you want to configure mobility.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Configure WLC Mobility**.

The **Configure Mobility Group** slide-in pane displays.

For more information, see Mobility configuration overview, on page 648.

Step 4 From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose from the existing mobility groups.

Information about the existing mobility peers is loaded from the intent available in Catalyst Center.

Note If you choose the default mobility group from the drop-down list, you cannot add mobility peers.

Step 5 In the **RF Group Name** field, enter a name for the RF group.

Step 6 To enable Datagram Transport Layer Security (DTLS) data encryption, click the **Data Link Encryption** button on.

Step 7 To enable or disable Cipher configuration for mobility, use the **DTLS High Cipher Only** toggle button.

Cipher configuration is applicable for Cisco Catalyst 9800 Series Wireless Controller Release 17.5 or later. You must manually reboot the device for changes to take effect.

Step 8 To manually reboot the device after making changes in the DTLS cipher configuration to take effect after provision, enable the **Restart for DTLS Ciphers to take effect** toggle button.

Step 9 Under **Mobility Peers**, click **Add** to configure a mobility peer. You can add a maximum of 24 peer devices to a mobility group.

Step 10 In the **Add Mobility Peer** slide-in pane, do this configuration:

a) Choose one of these types of mobility peers:

- To include mobility peers that are managed by Catalyst Center, click **Managed WLC**.
- To include mobility peers that are not managed by Catalyst Center, click **External WLC**.

b) If you choose **Managed WLC**, from the **Device Name** drop-down list, choose the controller.

After the device is provisioned, Catalyst Center creates a mobility group in the device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.

c) If you choose **External WLC**, do this configuration:

- In the **Device Name** field, enter the device name.
- (Optional) From the **Device Series** drop-down list, choose the device series.
- In the **Private IPv4/IPv6 Address** field, enter the private IPv4 or IPv6 address.
- (Optional) In the **Public IPv4/IPv6 Address** field, enter the public IPv4 or IPv6 address.
- In the **MAC Address** field, enter the MAC address of the device.
- In the **Mobility Group Name** field, enter the mobility group name.
- (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

Note This field is available only for Cisco Catalyst 9800-CL Wireless Controller.

d) Click **Save**.

Step 11 Click **Configure Mobility**.

Step 12 (Optional) You can reset the mobility group name and the RF group name using one of these methods:

- In the **Configure Mobility Group** slide-in pane, choose **default** from the **Mobility Group Name** drop-down list.
- In the **Configure Mobility Group** slide-in pane, click **Reset Mobility**.

This step automatically sets the **RF Group Name** to **default** and removes all peers. After you provision, the mobility on the device is set and the device is removed from all other peers.

Step 13 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 14 On the **Tasks** window, monitor the task deployment.

Configure AP Impersonation

Catalyst Center allows you to enable or disable AP Impersonation. AP Impersonation is a global setting that provides a quick and effective means to detect and report phishing incidents. AP Impersonation is supported for Catalyst 9800 Controllers.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click **Wireless** > **Security Settings**.

Step 3 In the left hierarchy tree, **Global** is selected by default. Expand the Global site and select the desired site, building, or floor.

Note The sites, buildings, and floors inherit the settings from the global level.

Step 4 Click the **AP Impersonation** tab.

Step 5 Check the **Enable AP Impersonation** check box to enable AP Impersonation.

Step 6 Select the type: **Auth IE** or **Infra MFP**.

Note **Infra MFP** type is selected by default.

Step 7 Click **Save**.

Step 8 (Optional) To disable the AP Impersonation, uncheck the **Enable AP Impersonation** check box.

About DTLS Ciphersuites

Ciphersuites are a set of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.

You can configure multiple DTLS (Data Datagram Transport Layer Security) Ciphersuites on Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, and Cisco Embedded Wireless Controller on Catalyst Access Points platforms running Release 17.5 or later.

Configure Multiple DTLS Ciphersuites

You can configure DTLS Ciphersuites either at the global level or site level.

Before you begin

- Make sure that the Device Controllability feature is enabled on the **System** > **Settings** > **Device Settings** > **Device Controllability** window.
- Discover Cisco Catalyst 9800 Series Wireless Controllers in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings** > **Wireless**.

Step 2 From the left hierarchy tree, select **Global** to configure all sites with the same DTLS Ciphersuite configuration.

From the left hierarchy tree, select a site to configure DTLS Ciphersuites at the site level. The DTLS Ciphersuite configuration will be pushed to the controller available on that particular site.

Step 3 Click **Security Settings**.

Step 4 Click the **Configure DTLS Ciphersuites** tab.

Step 5 Uncheck the **Skip DTLS Ciphersuite Config** check box to configure Ciphersuites as part of Device Controllability.

Step 6 Configure either default Ciphersuites or custom Ciphersuites.

By default, the **Default** Ciphersuite is selected.

The Default Ciphersuite box shows the list of default Ciphersuites and these Ciphersuites are configured as default on the device. You cannot change the priority of these default ciphersuites.

Step 7 To configure custom Ciphersuites, click the **Custom** button.

Custom Ciphersuite overrides the default Ciphersuites with priority.

Step 8 From the **Version** drop-down list, choose the DTLS version.

Based on the DTLS version, Catalyst Center shows the available Ciphersuites.

Step 9 Click the blue toggle button next to the Ciphersuite if you do not want to apply any of the Ciphersuites.

Step 10 To change the priority of Ciphersuites, drag each Ciphersuite.

Step 11 Click **Save**.

The message `DTLS Ciphersuite Config Saved successfully` is displayed.

Step 12 To apply the Ciphersuite configuration, you must provision the device.

For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

About N+1 Rolling AP Upgrade

The Rolling AP Upgrade feature is supported on the Cisco Catalyst 9800 Series Wireless Controller in an N+1 HA setup. This feature helps you upgrade software images on the APs associated with the Cisco Catalyst 9800 Series Wireless Controller in your wireless LAN network. To achieve the zero downtime, it is possible to upgrade APs in a staggered way using the N+1 Rolling AP Upgrade feature.

The primary controller identifies the candidate APs through the radio resource management neighbor AP map. The upgrade process starts with the software image downloading to the primary controller while the image is predownloaded to the candidate APs. After the candidate APs have been upgraded and rebooted, they join the secondary controller in a staggered manner. After all the APs have joined the secondary controller, the primary controller reboots. The APs rejoin the primary controller in a staggered manner after it is rebooted.

Here are the prerequisites for configuring the Rolling AP Upgrade feature:

- An N+1 HA setup with two wireless controllers, one as the primary controller and the other one as the secondary.
- The primary and the N+1 controllers have the same configuration and manage the same location in the network.
- The N+1 controller is already running the Golden image so that Rolling AP Upgrade works with zero downtime.

  Golden images are standardized images for network devices and Catalyst Center automatically downloads the images from cisco.com. Image standardization helps in device security and optimal device performance.
- The N+1 controller is reachable and in **Managed** state in Catalyst Center.
- Both the controllers are part of the same mobility group, and a mobility tunnel is established between the primary and N+1 controller. The upgrade information between the primary and N+1 controllers are exchanged through the mobility tunnel.

Note If you have a cyclic N+1 HA deployment, where *wireless controller 1* is N+1 for *wireless controller 2* and *wireless controller 2* is N+1 for *wireless controller 1*, you cannot run Rolling AP Upgrade on both devices. Instead, one controller must go through a normal upgrade. You can run Rolling AP Upgrade on the other controller after the first controller is upgraded without the rolling AP upgrade.

Workflow to Configure a Rolling AP Upgrade

This procedure shows how to configure a Rolling AP Upgrade on Cisco Catalyst 9800 Series Wireless Controllers.

Note N+1 Rolling AP Upgrade is supported on fabric and nonfabric deployments.

Procedure

Step 1 Install Catalyst Center.

For more information, see the *Cisco Catalyst Center Installation Guide*.

Step 2 Log in to the Catalyst Center GUI and verify that the applications you need are in the **Running** state.

From the main menu, choose **System** > **Software Updates** > **Installed Apps**.

Step 3 Discover the wireless controller using the Discovery feature.

You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations on network devices.

For more information, see Discover your network using CDP, on page 66 or Discover your network using an IP address range or CIDR, on page 68.

Step 4 Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.

For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.

You must wait for devices to move to a **Managed** state.

Step 5 Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Catalyst Center.

To import and upload an existing network hierarchy, see Import your site hierarchy to Catalyst Center, on page 233.

To create a new network hierarchy, see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

Step 6 Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

For more information, see Work with APs on a floor map, on page 256.

Step 7 Provision the primary controller with the primary managed AP location, Rolling AP Upgrade enabled, and mobility group configured with the secondary controller as its peer.

To do this, choose **Provision** > **Network Devices** > **Inventory**, and check the check box next to the primary controller name.

Step 8 Configure the N+1 controller as the mobility peer in the Mobility Group configuration.

For more information, see Mobility configuration overview, on page 648.

Step 9 Provision the N+1 HA controller by configuring the primary controller's primary managed AP location as the N+1 controller's secondary managed AP location. This configures the secondary controller as the N+1 controller.

For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 10 Provision the APs that are associated with the primary controller.

Step 11 Import the software images to the repository.

For more information, see Import a software image, on page 539.

Step 12 Assign the software image to a device family.

For more information, see Manage software image assignment for a device family, on page 540.

Step 13 Mark the software image as Golden by clicking the star for a device family or a device role.

For more information, see Mark a software image as standard, on page 545.

Step 14 Before upgrading the image, make sure that the image readiness checks are successful for both devices.

Also make sure that the status of the **N+1 Device Check** and the **Mobility Tunnel Check** has a green tick mark.

- To do the image update readiness check, choose **Provision** > **Network Devices** > **Software Images**.
- From the **Focus** drop-down list, choose **Software Images**. Select the device whose image you want to upgrade.
- If the prechecks are successful for a device, the **Status** link in the **Image Precheck Status** column has a green tick mark. If any of the upgrade readiness prechecks fail for a device, the Image Precheck Status link has a red mark, and you cannot update the OS image for that device. Click the **Status** link and correct any errors before proceeding.

Step 15 Initiate the upgrade on primary controller.

Step 16 On the **Software Images** window, check the check box next to the primary controller.

Step 17 From the **Actions** drop-down list, choose **Software Image** > **Update Image**.

For more information, see Provision a software image, on page 551.

Step 18 To monitor the progress of the image upgrade, click **In Progress** in the **Software Image** column.

The **Device Status** window displays this information:

- **Distribution Operation**: Provides information about the image distribution process. The image gets copied from Catalyst Center to the primary device. The activate operation starts after the distribution process is complete.
- **Activate Operation**: Provides the activate operation details. The Rolling AP Upgrade starts during this process.
- **Rolling AP Upgrade Operation**: Provides a summary of the Rolling AP Upgrade, such as whether the Rolling AP Upgrade task is complete, the number of APs pending, the number of rebooting APs, and the number of APs that have joined the N+1 controller.

  Click **View AP Status** to view details about the primary controller, N+1 controller, device names, current status, and iterations.

Provision a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to provision a Cisco Catalyst 9800 Series Wireless Controller.

Before you begin

Ensure that you have completed the steps in Configure a Cisco Catalyst 9800 Series Wireless Controller in Catalyst Center, on page 636.

To share the wireless controller across multiple fabric sites, ensure that you have completed the requirements. For more information, refer to Shared wireless controllers for multiple fabric sites, on page 1080.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 In the **Devices** table, check the check box next to the wireless controller name that you want to provision.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 4 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, click the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, refer to "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue with device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box and select a different wireless controller.

Step 5 In the **Assign Site** window, assign a site to the wireless controller.

a) Click **Choose a Site**.

b) In the **Choose a site** slide-in pane, click the site name that you want to assign to the wireless controller, and click **Save**.

c) Click **Next**.

Step 6 In the **Configuration** window, select a role for the Cisco Catalyst 9800 Series Wireless Controller: **Active Main WLC** or **Anchor**.

Step 7 Select the managed AP location.

- Click **Select Primary Managed AP Locations** to select the managed AP location for the primary controller.
- Click **Select Secondary Managed AP Locations** to select the managed AP location for the secondary controller.

Step 8 Select either a parent site or individual sites for the managed AP locations, and click **Save**.

If you select a parent site, all the children under the parent site are also chosen. You can uncheck the check box to deselect a child site.

Note The inheritance of managed AP locations allows you to automatically select a site along with the buildings and floors under that particular site. One site is managed by only one wireless controller.

Step 9 (Optional) Check the **AP Authorization List** check box to select the authorization list for AP authorization, and then configure the AP authorization settings.

Note This check box is displayed only if an AP authorization list is available. For more information about the AP authorization list, refer to Create an AP authorization list, on page 417.

- From the **AP Authorization List Name** drop-down list, select an AP authorization list. Based on the content of the AP authorization list, Catalyst Center displays a message indicating the corresponding primary authorization type and failback mechanism.
- (Optional) To view the entries for the selected AP authorization list, click **View Entries**.
- If the wireless controller manages both mesh and nonmesh APs, Catalyst Center displays the **Authorize Only Mesh Access Points** and **Authorize All Access Points** check boxes.

  To enable authorization for only mesh APs, check the **Authorize Only Mesh Access Points** check box.

  To enable authorization for all APs, check the **Authorize All Access Points** check box.

Step 10 For an active main wireless controller, configure the interface and VLAN details.

Step 11 (Optional) In the **Configure VLAN** area, configure VLAN settings.

You can configure up to eight IPv6 addresses and one IPv4 address for a dynamic interface. To configure dynamic interfaces, refer to Configure additional interfaces for a network profile, on page 478.

Note For the FlexConnect SSIDs, VLANs aren't automatically created on the Cisco Catalyst 9800 Series Wireless Controllers during provisioning. The interface and VLANs mapped to the wireless network profile are created on the Flex profile during AP provisioning.

Select the required VLAN and click **Edit**. In the **Configure VLAN** slide-in pane, complete these configurations:

a) (Optional) In the **IPv4** tab, enter data in these fields:

- **Interface IP Address**: Enter the IPv4 address for the interface.
- **Gateway IP Address**: Enter the gateway IPv4 address for the interface.
- **Subnet Mask (in bits)**: Enter the subnet mask details for the interface.

b) (Optional) In the **IPv6** tab, click **Add IPv6 Address** and complete these configurations:

- Enter the IPv6 address for the interface.
- From the **Prefix Length** drop-down list, choose a prefix length.

Step 12 (Optional) Check the **Skip AP Provision** check box to skip configuring the AP-related commands while provisioning the wireless controller.

For more information, refer to Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning, on page 1442.

Note When you reprovision the wireless controller, Catalyst Center skips configuring AP-related commands if the AP intent configuration does not change. You can use this check box to skip AP-related configurations when there are changes to the intent configuration.

For more information about the detected AP configuration changes, refer to Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning, on page 1442.

Step 13 (Optional) Check the **Rolling AP Upgrade** check box to enable the Rolling AP Upgrade feature in an N+1 HA setup.

(Optional) If you check this check box, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions.

For more information, refer to Workflow to Configure a Rolling AP Upgrade, on page 654.

Note If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

Step 14 (Optional) Check the **AP LSC Certificate Renewal** check box to renew the Locally Significant Certificate (LSC) for the associated APs before its expiry.

By default, the wireless controller renews the AP LSCs daily at 12:00 AM in a staggered manner.

If you check this check box, complete these configurations:

- From the **Renewal Profile** drop-down list, select an AP LSC renewal profile.

  To create an AP LSC renewal profile, refer to Create an AP LSC renewal profile, on page 419.

- (Optional) If you select an AP LSC renewal profile for staggered renewal, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

  Note If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

Step 15 (Optional) To make the wireless controller eligible for sharing with multiple fabric sites, check the **Share With Fabric Sites** check box, then choose the fabric sites where the wireless controller can be shared.

If sharing is already enabled on the wireless controller, click **Edit** to manage the remote fabric sites.

Note This feature is in beta.

In the **Edit Fabric Sites** slide-in pane, complete these configurations:

a) In **Step 1 of 2: Select Fabric Sites**, select the fabric sites where you want to share the wireless controller.

Catalyst Center lists the sites that are configured as the primary or secondary managed AP locations for this wireless controller.

b) Check the **Split Network Profiles for new shared Fabric Sites** to create site-specific network profile copy.

c) Click **Next**.

d) **Step 2 of 2: Resolve Network Profile Conflicts** lists the network profile conflicts for newly added fabric sites. For each conflict, review the current network profile, proposed **New Network Profile Name**, and **SSID and Policy Profile Mapping**. Edit the proposed names as needed, and click **Apply**.

Catalyst Center does not clone the custom policy tags, CLI templates, and feature templates associated with the profile during this step. Configure them manually after Catalyst Center creates the site-specific network profile copy.

e) After resolving all conflicts, click **Save**.

Note

- If the managed AP locations change after site selection, Catalyst Center displays a warning message. Review the site selection before provisioning.
- This step makes the wireless controller eligible for sharing with multiple fabric sites. To share the wireless controller, add it to each remote fabric site. For more information, refer to Configure a shared wireless controller for multiple fabric sites, on page 1083.

Step 16 Click **Next**.

Step 17 In the **Devices** pane of the **Feature Templates** window, select a feature template.

You can either search for a feature template by entering its name in the **Find** field, or expand the device and select a feature template. The chosen feature template is displayed in the right pane.

Step 18 Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the feature template.

You can't edit all the configurations in this step.

Step 19 After making the necessary changes, click **Apply**.

Step 20 Click **Next**.

Step 21 In the **Devices** pane of the **Advanced Configuration** window, search for the device or template.

Step 22 In the **wlanid** field, enter a value for the predefined template variable, and click **Next**.

Step 23 In the **Summary** window, review the configuration settings, and click **Next**.

Step 24 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 25 On the **Tasks** window, monitor the task deployment.

Note When you provision the wireless controller, Catalyst Center pushes the configuration to the wireless controller and configures it based on the network intent.

During the reprovisioning, if there are any out-of-band configurations on the wireless controller that are a part of the network intent or conflicting with the configurations being pushed by Catalyst Center, Catalyst Center overwrites the out-of-band configurations on the wireless controller with the network intent configuration.

The selective AP group Resource Facing Service (RFS) translate feature optimizes reprovisioning for AP-related configurations (such as AP tag mapping, RF tags, and flex or RF profiles). Out-of-band changes to AP-related configurations are not automatically corrected during reprovisioning unless a compliance report explicitly flags them. To correct the AP-related out-of-band configurations to match your network intent, perform a wireless controller resynchronization and compliance run. For example, if you manually update the static AP tag mapping:

- With resynchronization and compliance run, the manual change is corrected to match the intent configuration.
- Without resynchronization and compliance run, the manual change is not corrected and only the new intent changes are applied.

To disable the selective AP group RFS translate feature, contact Cisco Technical Assistance Center (TAC).

For all the configurations that are supported through the network intent on Catalyst Center, we recommend that you use them instead of out-of-band configurations.

Step 26 Verify the configurations that are pushed from Catalyst Center to the device using the show commands on the wireless controller.

- **#show wlan summary**
- **#show run | sec line**
- **#show running-configuration**

Step 27 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 28 In the **Inventory** window, from the **Focus** drop-down list, select **Provision**.

Step 29 Under the **Provisioning Status** column, click the **See Details** link of a corresponding device to view information about network intent or a list of actions.

Step 30 In the device slide-in pane, click **See Details** under **Device Provisioning**.

Step 31 Click **View Details** under **Deployment of network intent**, and click the device name.

Step 32 Click and expand the device name.

Step 33 Expand the **Configuration Summary** area to view the operation details, feature name, and management capability.

The configuration summary also displays any error (with failure reasons) that occurred while provisioning the device.

Step 34 Expand the **Provision Summary** area to view details of the configuration that is sent to the device.

Step 35 Provision the AP.

Day-zero workflow for Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-APs) is the next-generation Wi-Fi solution, which combines the Cisco Catalyst 9800 Series Wireless Controller with Cisco Catalyst 9100 Series Access Points, creating the best-in-class wireless experience for the evolving and growing organization.

Before you begin

- Design your network hierarchy with sites, buildings, floors, and so on.

  For more information, see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS for the site where you want to claim the device.

  For more information, see Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, and Add global SNMPv3 credentials, on page 325.

- Create wireless SSIDs, wireless interfaces, and wireless Radio Frequency profiles.

  For more information, see Create SSIDs for an enterprise wireless network, on page 351, Create SSIDs for a guest wireless network, on page 366, Create a wireless interface, on page 381, and Create a wireless radio frequency profile, on page 383.

Note For Cisco Embedded Wireless Controller on Catalyst Access Points, only Flex-based SSID creation is supported.

- Configure the DHCP server with Option #43 on the switch where the Cisco Embedded Wireless Controller on Catalyst Access Points is connected. This IP address is IP address of the Catalyst Center Plug and Play (PnP) server. Using this IP address, the APs contact the PnP server, but remain in the **Unclaimed** state.

- Make sure that you have the Cisco Embedded Wireless Controller on Catalyst Access Points in the inventory. If not, discover them using the Discovery feature. For more information, see Discover your network using CDP, on page 66, Discover your network using an IP address range or CIDR, on page 68, and About Inventory, on page 78.

- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

The Cisco Embedded Wireless Controller on Catalyst Access Points is available in multiple form factors:

- Cisco Embedded Wireless Controller on Catalyst 9115AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9117AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9120AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9130AX Access Points

Procedure

Step 1 The Cisco Embedded Wireless Controller on Catalyst Access Points contacts the DHCP server.

In response, the DHCP server provides the IP address along with Option #43, which contains the IP address of the Cisco Plug and Play server.

Step 2 Based on Option #43, the Cisco Embedded Wireless Controller on Catalyst Access Points turns on the Plug and Play agent and contacts the Catalyst Center Plug and Play server.



Note If you have a set of Cisco Embedded Wireless Controller on Catalyst Access Points in the network, they go through an internal protocol. The protocol selects one Cisco Embedded Wireless Controller on Catalyst Access Points, which is configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

Step 3 Find the unclaimed Cisco Embedded Wireless Controller on Catalyst Access Points in the **Provision** > **Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the onboarding status to become **Initialized** under the **Onboarding State** column.

Step 4 To claim the Cisco Embedded Wireless Controller on Catalyst Access Points, check the check box next to the AP device name.

Step 5 Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window displays.

Step 6 In the **Assign Site** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

Step 7 Click **Next**.

Step 8 In the **Assign Configuration** window, to configure a device, click the corresponding **Assign** option.

Step 9 In the **Configuration for device name** slide-in pane, do these tasks:

- In the **Wireless Management IP** field, enter the wireless management IP address.

  The IP address must not be the same as the IP address that the AP uses for contacting the PnP server.

- In the **Subnet Mask** field, enter the subnet mask.
- In the **Gateway** field, enter the gateway IP address.

Step 10 Click **Save**.

Step 11 Click **Next**.

The **Summary** window displays.

Step 12 Click **Claim**.

After the Cisco Embedded Wireless Controller on Catalyst Access Points claim is successful, the configured wireless management address, subnet mask, and gateway are assigned to the Cisco Embedded Wireless Controller.

The claimed device is now listed on the **Provision** > **Inventory** window and moved to the **Managed** state. The device is automatically provisioned. After the provisioning is complete, you can view the device on the **Provisioned** tab of the **Provision** > **Plug and Play** window.

Configure and provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches

Supported hardware platforms

Device role	Platforms
Embedded Wireless Controller	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches
Fabric Edge	Cisco Catalyst 9300 Series Switches Cisco C9350 Series Smart Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches Cisco Catalyst 3600 Series Switches Cisco Catalyst 3850 Series Switches
APs	Cisco 802.11ac Wave 2 APs: • Cisco Aironet 1810 Series OfficeExtend Access Points • Cisco Aironet 1810W Series Access Points • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w Access Point • Cisco Aironet 1815m Access Point • Cisco 1830 Aironet Series Access Points • Cisco Aironet 1850 Series Access Points • Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points

Device role	Platforms
	Cisco 802.11ac Wave 1 APs • Cisco Aironet 1700 Series Access Points • Cisco Aironet 2700 Series Access Points • Cisco Aironet 3700 Series Access Points Cisco Catalyst 9105 Series Wi-Fi 6 Access Points Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Cisco Catalyst 9117 Series Wi-Fi 6 Access Points Cisco Catalyst 9120 Series Wi-Fi 6 Access Points Cisco Catalyst 9124 Series Wi-Fi 6 Access Points Cisco Catalyst 9130 Series Wi-Fi 6 Access Points Cisco Catalyst 9136 Series Wi-Fi 6 Access Points Cisco Catalyst Wireless 9136I Wi-Fi 6 Access Point Cisco Catalyst Wireless 9163E Wi-Fi 6 Access Point Cisco Catalyst Wireless 9166D Wi-Fi 6 Access Point Cisco Catalyst Wireless 9166I Wi-Fi 6 Access Point Cisco Catalyst Wireless 9162I Wi-Fi 6 Access Point Cisco Catalyst Wireless 9164I Wi-Fi 6 Access Point Cisco Catalyst Wireless 9167 Series Wi-Fi 6 Access Point Cisco Wireless 9171I Series Wi-Fi 7 Access Points Cisco Wireless 9172H Series Wi-Fi 7 Access Points Cisco Wireless 9172I Series Wi-Fi 7 Access Points Cisco Catalyst Wireless 9176 Series Wi-Fi 6 Access Point Cisco Catalyst 9176D1 Series Wi-Fi 7 Access Points Cisco Catalyst 9176I Series Wi-Fi 7 Access Points Cisco Wireless 9177D Series Wi-Fi 7 Access Points Cisco Wireless 9177E Series Wi-Fi 7 Access Points Cisco Wireless 9177I Series Wi-Fi 7 Access Points Cisco Catalyst Wireless 9178 Series Wi-Fi 6 Access Point Cisco Catalyst 9178I Series Wi-Fi 7 Access Points

Preconfiguration

On Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, make sure that these commands are present if the switch is already configured with **aaa new-model**:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

This is required for NETCONF configuration. These configurations are not required if you are using automated underlay for provisioning.

Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches

1. Install Catalyst Center.

   For more information, see the Cisco Catalyst Center Installation Guide.

2. Log in to the Catalyst Center GUI and verify that the applications you need are in the **Running** state.

   From the main menu, choose **System** > **Software Updates** > **Installed Apps**.

3. Integrate Cisco Identity Services Engine with Catalyst Center. After Cisco ISE is registered with Catalyst Center, any device that Catalyst Center discovers, along with relevant configurations and other data, is pushed to Cisco ISE.

4. Discover Cisco Catalyst 9000 Series Switches and the edge switches.

   You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.

   Do not enable NETCONF to discover the edge switches.

   For more information, see Discover your network using CDP, on page 66 and Discover your network using an IP address range or CIDR, on page 68.

   Change the **Preferred Management IP** to **Use Loopback**.

5. Make sure that the devices appear in the device inventory and are in **Managed** state.

   For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.

   Ensure that the devices are in the **Managed** state.

6. Design your network hierarchy, which represents your network's geographical location. You can create sites, buildings, and floors so that later you can easily identify where to apply the design settings or configurations.

   You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Catalyst Center.

   To import and upload an existing network hierarchy, see the Import your site hierarchy to Catalyst Center, on page 233.

   To create a new network hierarchy, see the Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

7. For a nonfabric network, add and position APs on a floor map to get heatmap visualization during the design phase.

For a fabric network, you cannot place APs on a floor map during the design time. The APs are onboarded after adding devices to a fabric network.

For more information, see Work with APs on a floor map, on page 256.

8. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network.

   You can configure up to six AAA servers on the **Wireless** window during the SSID creation.

   For more information, see Network settings overview, on page 317, Configure global network servers, on page 321, and Add AAA server.

9. Configure device credentials, such as CLI, SNMP, and HTTPs.

   For more information, see Configure global device credentials, on page 323, Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, Add global SNMPv3 credentials, on page 325, and Add global HTTPS credentials, on page 327.

10. Configure IP address pools at the global level.

    To configure an IP address pool, see Configure IP address pools, on page 337.

    To reserve an IP address pool for the building that you are provisioning, see Reserve IP Address Pools.

11. Create enterprise and guest wireless networks. Define the global wireless settings once, and then Catalyst Center pushes the configurations to various devices across geographical locations.

    Designing a wireless network is a two-step process. First, you must create SSIDs on the **Wireless** window. Then, associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

    For more information, see Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

12. Configure the backhaul settings.

13. On the **Policy** window, do this configuration:

    - Create a virtual network. The virtual network segments your physical network into multiple logical networks.
    - Create a group-based access control policy, and add a contract. For more information, see Create group-based access control policy, on page 1192.

14. Provision Cisco Catalyst 9000 Series Switches and the edge node switches with the configurations added during the design phase.

    - Create a fabric site.
    - Add devices to the fabric network by creating a CP+Border+Edge or CP+Border.
    - Enable embedded wireless capabilities on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.
    - Onboard APs in the fabric site.

    For more information, see Provision SD-Access LISP Fabric Network, on page 1005.

After the devices are deployed successfully, the deploy status changes from **Configuring** to **Success**.

Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches

Before you begin

Before provisioning a Cisco Catalyst 9800 Embedded Wireless Controller on Catalyst 9000 Series Switches, ensure that you have completed the steps in Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches, on page 666.

This procedure explains how to provision embedded wireless on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500H Series Switches.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window display with the discovered devices listed.

Step 2 Check the check box next to the Catalyst 9000 Series Switch device and the edge switch that you want to associate to a site.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Assign Device to Site**. Assign the devices to a site. For more information, see Assign an unprovisioned device to a site, on page 156.
The next step is to provision the Catalyst 9000 Series Switch and the edge node with the configurations that were added during the design phase.

Step 4 In the **Provision** > **Inventory** window, check the check box next to the device name that you want to provision.

a) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
b) Click **Next**.
c) In the **Summary** window, review the configuration, and click **Next**.
d) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

e) On the **Tasks** window, monitor the task deployment.

Step 5 To provision the edge switch, check the check box next to the edge switch that you want to provision.

a) From the **Actions** drop-down list, choose **Provision**.
b) Click **Next**.
c) In the **Summary** window, verify the configurations, and click **Deploy**.

After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 6 To add devices to a fabric site, click the menu icon and choose **Provision** > **Fabric Sites**.

Step 7 Create a fabric site. For more information, see Add a fabric site, on page 1018.

Step 8 Add an IP transit network.

Step 9 Add devices and associate virtual networks to a fabric site.

Step 10 Add the Cisco Catalyst 9000 Series Switch as a control plane, a border node, and an edge node or a control plane and a border node.

a) Click the device and choose **Add as CP+Border+Edge** or **Add as CP+Border**.
b) Click the edge node and choose **Add to Fabric**.
c) Click **Save**.

Step 11 To enable embedded wireless on the device, click the device that is added as a **Edge**, **CP+Border+Edge** or **CP+Border**, and click the **Embedded Wireless LAN Controller** toggle button.

a) If you haven't installed the wireless package on Cisco Catalyst 9000 Series Switches before enabling the wireless capability, Catalyst Center displays a warning message indicating that the embedded wireless controller software image is necessary for enabling the capability. In the warning dialog box, click **OK** to install the image manually.
b) On the **Download Image** window, click **Choose File** to navigate to a software image stored locally, or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.
c) Click **Import**.

   The progress of the image import is displayed. To exit the window, and view the progress of the import and schedule the installation later, click **Close**.

d) After the image import is complete, under **Schedule Image Installation** on the **Download Image** window, choose one of these options:

   - **Now**: Immediately install the image.
   - **Later**: Schedule the image installation for a later date or time.

e) In the **Task Name** field, update the task name, if required.
f) If you chose **Later**, do these tasks:

   - Under **Start Date/Time**, specify a start date and time for the image installation.
   - To use the default site time zone for the image installation, check the **Site Settings** check box. To select a time zone, uncheck the **Site Settings** check box and choose a time zone from the drop-down list.

g) Click **Apply**.

   To view the status of image installation, go to the **Activities** > **Tasks** window and open the relevant work item.

h) After the embedded wireless controller software image is distributed and activated on the switch, resynchronize the device using the **Provision** > **Inventory** > **Resync** option.

Step 12 On the **Manage Scope** window, do these tasks:

- Under the **Primary** tab, check the check box next to the required site name.
- Under the **Secondary** tab, check the check box next to the required site name.

You can select either a parent site or individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

You can also use the **Search Hierarchy** search field or the filter icon to find a site.

Step 13 Click **Next**.

Step 14 On the **Advanced** window, configure the required settings.

- To enable the Rolling AP Upgrade feature, check the **Rolling AP Upgrade** check box.

  (Optional) If you check this check box, from the **AP Reboot Percentage** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

- To renew the Locally Significant Certificate (LSC) for the associated APs before its expiry, check the **AP LSC Certificate Renewal** check box.

  If you check this check box, complete these configurations:

  - From the **Renewal Profile** drop-down list, select an AP LSC renewal profile.

    To create an AP LSC renewal profile, see Create an AP LSC renewal profile, on page 419.

  - (Optional) If you select an AP LSC renewal profile for staggered renewal, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.



Note If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

Step 15 Click **Next**.

Step 16 On the **Summary** window, review the configuration settings, and click **Save**.

Step 17 On the **Modify Fabric** step, click **Now** to commit the changes, and click **Apply** to apply the configurations.
The next step is to onboard APs in a fabric site.

Step 18 In the Catalyst Center GUI, click the menu icon and choose **Provision** > **Fabric Sites**.

A list of fabric sites displays.

Step 19 Select the fabric site that was created, and click the **Host Onboarding** tab to enable IP pool for APs.

Step 20 Select the authentication template that is applied for devices in the fabric site. Then, click **Save**.

Step 21 Under **Virtual Networks**, click **INFRA_VN** to associate one or more IP pools with the selected virtual network.

Step 22 Under **Virtual Network**, click the guest virtual networks to associate IP pools for the selected guest virtual network.

Step 23 Check the **IP Pool Name** check box that was created for APs during the design phase.

Step 24 Click **Update** to save the setting.

The AP gets the IP address from the specified pool, which is associated with the AP VLAN and registers with the wireless controller through one of the discovery methods.

Step 25 Specify wireless SSIDs within the network that hosts can access. Under the **Wireless SSID** section, select the guest or enterprise SSIDs and assign address pools, and click **Save**.

Step 26 Manually trigger resynchronization by choosing **Inventory** > **Resync** to see the APs on Catalyst Center for embedded wireless.
The discovered APs are now displayed under **Inventory** in the **Provision** window and the **Status** is displayed as **Not Provisioned**.

Step 27 Provision the AP.

For more information, see Provision Cisco APs on day 1, on page 627.

Step 28 Configure and deploy application policies. For more information, see Create an application policy, on page 1231, Deploy an application policy, on page 1237, and Edit an application policy, on page 1235.

Provision the Catalyst 9300 Series Switches and Cisco Catalyst 9500H Series Switches before deploying an application policy.

Two different policies with different business relevance for two different SSIDs don't work. The last deployed policy takes precedence when you're setting up the relevance.

Changing the default business relevance for an application doesn't work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

Renew AP LSC for a wireless device

Before you begin

Ensure that the device is running Cisco IOS XE Release 17.1.7.1 or later.

Use this procedure to renew the AP Locally Significant Certificate (LSC) for a wireless device before it expires.

You can renew the AP LSCs for these devices:

- Cisco Catalyst 9800 Series Wireless Controllers
- Wireless-capability-enabled switches

You can renew the certificates for APs that are due for renewal based on the due time, site tags, or manual selection.

Procedure

Step 1 Navigate to the device in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global**, and choose an area, building, or floor.
c) Select the device to renew the AP LSCs.

Step 2 From the **Actions** drop-down list, choose **Provision** > **Renew AP LSC Certificate**.

Step 3 In the **Renew Access Point Certificate** window, complete these configurations:

a) Select an option for renewing the AP LSCs.

Table 51: AP selection options

Option	Description
All APs due for certificate renewal	Renews the certificates for all APs that are due for renewal based on the number of days before expiry. In the **Due Time** field, enter the number of days before AP LSC expiry. The valid range is 0 to 60 days.

Option	Description
APs configured with selected site tags and due for certificate renewal	Renews the certificates for all APs that are due for renewal based on the site tags. • From the **Site tags** drop-down list, select one or more site tags. • In the **Due Time** field, enter the number of days before AP LSC expiry. The valid range is 0 to 60 days.
Manually select APs	Renews the certificates for all APs that are due for renewal based on your selection. In the table, select the required APs. **Note** You can search for APs using the search field for each column in the table. In the search field, manually enter a value, and press **Enter**. The search results display the corresponding APs with value highlighted throughout the column.

b) Click **Submit**.

Step 4 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 5 On the **Tasks** window, monitor the task deployment.

Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Catalyst Center allows you to customize individual features or parameters on Cisco Catalyst 9800 Series Wireless Controllers using the Per-Device Configuration feature. Using Per-Device Configuration, you can create, edit, clone, and delete the device-level configurations for a wireless controller.

You can use these configurations to onboard new wireless controllers to Catalyst Center and manage their configurations. You can also manage the APs associated with these wireless controllers.

Default status

By default, the Per-Device Configuration feature is disabled on Catalyst Center. To enable the configurations, see Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 674.

Limitations

- Per-Device Configuration isn't supported for
  - wireless controllers that were previously added to Catalyst Center and are using intent-based wireless network configurations with site-based network profiles (for these wireless controllers, Per-Device Configuration is available in read-only mode), and
  - SD-Access wireless configurations.
- For AI-Enhanced RRM configurations, Per-Device Configuration is supported for only the Assurance use case with the **Enable Without Device Provisioning** deployment type.

Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

- Ensure that the wireless controller is running Cisco IOS XE Release 17.12 or later.
- Add the wireless controller to Catalyst Center.
  - You can add a single device manually and add multiple devices using discovery or by importing a CSV file on the **Inventory** window. For more information, see Add devices to the Catalyst Center Inventory, on page 128.
  - You can migrate the devices from Cisco Prime Infrastructure using the Prime Data Migration Tool (PDMT). For more information, see *Cisco Prime Infrastructure to Cisco Catalyst Center Prime Data Migration Guide*.
- Ensure that the devices are displayed on the **Inventory** window and are in the **Managed** state.

  For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.
- Design your network hierarchy by adding areas, buildings, and floors. This structure makes it easier to identify sites for applying configurations later.

  You can either
  - create a network hierarchy (see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242), or
  - import an existing network hierarchy into Catalyst Center if you have it on Cisco Prime Infrastructure (see Import your site hierarchy to Catalyst Center, on page 233).
- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

  For more information, see Work with APs on a floor map, on page 256.
- Ensure that the country codes are configured.

For more information, see About wireless devices and country codes, on page 617.

Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to enable the Per-Device Configuration feature for a Cisco Catalyst 9800 Series Wireless Controller.

Note If the wireless controller is managed using intent-based wireless network configurations with site-based network profiles, Per-Device Configuration can be used in read-only mode for the wireless controllers.

Before you begin

Ensure that the prerequisites are met. See Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 673.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 From the top-right corner of the device details window, click **Enable Per-Device Configuration**.

Step 4 In the **Per-device configuration** dialog box, view the details and click **Enable**.

What to do next

Ensure that the wireless controller is resynchronized before performing other operations. For more information on manually resynchronizing the wireless controller, see Resynchronize device information, on page 182.

Configure per-device features for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure and provision individual features using Per-Device Configuration for a wireless controller.

Note If you make any configuration changes outside of Catalyst Center (for example, through CLI or WebUI), these changes are detected and imported during the next inventory synchronization. This process may lead to conflicts. To maintain consistency and ensure predictable network behavior, we recommend that you use Catalyst Center for all supported configuration changes.

Before you begin

Ensure that

- the prerequisites are met (see Prerequisites for Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 673) and
- Per-Device Configuration is enabled on the wireless controller (see Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 674).

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 (Optional) From the top-right corner of the device details window, click **Manage APs** to modify the AP configuration for the APs associated with the wireless controller.

For more information, see Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller, on page 676.

Step 4 In the **Configuration** tab, configure and provision the required features for the wireless controller.

- **SSID**: See SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 682.
- **RF**: See RF configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 714.
- **AP**: See AP configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 728.
- **Tag Mapping**: See Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 761.
- **Security**: See Security configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 768.
- **Global Wireless**: See Global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 835.
- **Services**: See Service configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 907.
- **Layer 2**: See Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 930.
- **Network Settings**: See Network settings for a Cisco Catalyst 9800 Series Wireless Controller, on page 944.
- **Layer 3**: See Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 963.
- **Administration**: See Administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 965.

To search for a configuration, in the left pane of the device details window, click the **Search Features** field, and enter the name of the configuration.

Note The available configurations and their options can vary based on the Cisco IOS XE release running on the wireless controller.

Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to manage the APs associated with a wireless controller through Per-Device Configuration. You can configure the tags (site tag, policy tag, and RF tag) and tag-mapping profiles for APs associated with a wireless controller.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 From the top-right corner of the device details window, click **Manage APs**.

Step 4 (Optional) In the **Access Points** slide-in pane, edit the AP configuration set under **Operational Access Points**.

a. Check the check box next to the required AP names.

b. Click **Edit AP Configuration Set**.

The **Edit AP Configuration Set** slide-in pane opens.

c. From the **Policy Tag** drop-down list, choose a policy tag.

d. From the **Site Tag** drop-down list, choose a site tag.

e. From the **RF Tag** drop-down list, choose an RF tag.

f. Complete Step 7, on page 677 through Step 9, on page 677 to provision the configuration.

Step 5 (Optional) Assign APs to a site.

a. Check the check box next to the required AP names.

b. Click **Assign AP to Site**.

The **Assign AP to Site** slide-in pane opens.

c. Choose the required site.

Note You can either search for a site by entering its name in the **Search** field or expand **Global** to choose the site.

d. Click **Assign**.

Step 6 (Optional) Click **Configure AP and Radio Parameters** to configure the AP and radio parameters.

For more information, see Configure APs, on page 1382.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Customize table settings for Per-Device Configuration

Use this procedure to customize the Per-Device Configuration table settings for a feature if the device details window displays a table.

Note This procedure isn’t applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, click the required settings.

Step 4 In the corresponding configuration table, click the gear icon at the top-right corner.
The **Table Settings** slide-in pane opens.

Step 5 Click **Table Appearance** to adjust the table density and table striping.
a) Under **Table Density**, choose an option: **Default** or **Compact**
b) To apply table striping, click the toggle button under **Table Striping**.
c) Click **Apply**.

Step 6 (Optional) To reset the table settings, click **Reset All Settings**.

Edit a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to edit the Per-Device Configuration for a feature if the device details window displays a table.

Note This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, click the required per-device feature.

Step 4 Check the check box next to the configuration that you want to edit.

Step 5 Hover your cursor over **Actions** and click **Edit**.

Step 6 In the slide-in pane, edit the required configurations.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Clone a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to clone the Per-Device Configuration for a feature if the device details window displays a table.

Note This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, click the required per-device feature.

Step 4 Check the check box next to the configuration that you want to clone.

Step 5 Hover your cursor over **Actions** and click **Clone**.

Step 6 In the slide-in pane, complete the required configurations.

Step 7 (Optional) Edit the other necessary configurations.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Clone a Per-Device Configuration from another Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to clone the Per-Device Configuration from another Cisco Catalyst 9800 Series Wireless Controller for these features:

- WLAN profile
- Policy profile
- AP join profile
- RF profile
- Flex profile
- Site tag

If you clone a configuration from a wireless controller running a different Cisco IOS XE Release, some options might be unavailable or incorrect. Catalyst Center chooses a default that applies to your wireless controller in these cases. Verify the values before proceeding.

Note If the wireless controller from which you are cloning the configurations is encrypted with a master key, you must configure a password (clear text or encrypted) during the cloning process for WLAN profiles and AP join profiles to enable successful provisioning.

Before you begin

Ensure that the wireless controller that you want to clone is already added to Catalyst Center and is in the Managed state.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, click the corresponding per-device feature.

Step 4 Click **Clone from another WLC**.

Step 5 In the slide-in pane, complete these steps:

a) From the drop-down list, choose the wireless controller from which you want to clone the configuration.

The list of configurations associated with the chosen wireless controller is displayed.

b) Choose the required configuration.

c) Click **Clone**.

Step 6 In the warning dialog box, click **OK**.

Step 7 A slide-in pane displays the cloned configurations from the selected wireless controller.

Note Cloning a feature copies the configuration from the source wireless controller. Review the configurations before applying them to ensure compatibility with the target wireless controller.

Step 8 Edit the required configurations.

Note A warning icon on the left pane indicates any configuration conflicts. Review the conflict, then select an appropriate value to continue to the next window.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Delete a Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to delete the Per-Device Configuration for a feature if the device details window displays a table.

Note This procedure isn't applicable if the window doesn't display a table for the feature, such as **Airtime Fairness**.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, click the required per-device feature.

Step 4 Check the check box next to the configurations that you want to delete.

Step 5 Hover your cursor over **Actions** and click **Delete**.

Step 6 In the dialog box, click **Yes**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device SSID configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a WLAN profile for a wireless controller and provision it. WLAN profiles configure the Wi-Fi settings, enabling users to connect to a wireless network.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **SSID** and click **WLAN Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create WLAN Profile** slide-in pane, complete these configurations.

a) In the **Wireless Network Name (SSID)** field, enter a unique SSID name.

b) In the **WLAN ID** field, the WLAN ID is automatically populated based on the next available number.

If necessary, update the WLAN ID. The valid range is from 1 to 4096.

c) In the **WLAN Profile Name** field, the WLAN profile name is automatically populated based on the WLAN profile name.

If necessary, update the name.

Note Ensure that the WLAN profile name is unique and does not match any existing RLAN profile names. Otherwise, the WLAN profile creation task fails.

d) Under **SSID State**, use the toggle button to enable or disable the corresponding status.

- **Admin Status**: enable or disable the administrative status of the WLAN.

  If you disable this toggle button, the corresponding SSID isn't broadcast in the AP beacons.

- **Broadcast SSID**: enable or disable the visibility of the SSID to all the wireless clients within range.

e) Under **Wi-Fi 7 Compatibility**, view the Wi-Fi 7 compatibility information.

To view the details, click **Show Details**.

To ensure Wi-Fi 7 compatibility, in Step 6, on page 685, complete these configurations:

- enable WPA3.
- choose one of these supported combination of cipher and authentication key management:
  - AES and 802.1X-SHA256 or FT-802.1X

- GCMP256 and SAE-EXT-KEY, FT-SAE-EXT-KEY, or OWE
- GCMP256 and 802.1X-SHA256 or FT-802.1X
- GCMP256 and Suite-B-192

- set Protected Management Frame (PMF) to **Required** or **Optional**.

f) Under **Wi-Fi 7 Per Band Status**, view the per-band status for Wi-Fi 7 configuration.

To view the details for each band, click **Show Details**.

To enable Wi-Fi 7 per each band, complete these configurations:

- Enable the band under **Radio Policy**.
- Enable Global 11be for each band. For more information, refer to Configure high throughput parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 838.
- Enable the band in the Multi-Link Operation (MLO) group in the selected 802.11be profile. For more information, refer to Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 712.

g) Under **Radio Policy**, complete these configurations.

- The supported radio slots for each 802.11 band are listed. Click **Show Slot Configuration** to view the slot configuration for the corresponding bands.

Note In the slot configuration, if a check box is available next to a slot, you can use it to enable or disable the slot for the corresponding band.

- Use the **6 GHz**, **5 GHz**, and **2.4 GHz** toggle buttons to enable or disable the radio policy for the corresponding band.

Note The 6-GHz band is supported only when

- WPA2 is disabled, and
- WPA3, protected management frame, and 802.11ax configurations are enabled.

- From the **Bg Policy** drop-down list, choose a policy.

Note This drop-down list is available only when you enable the **2.4 GHz** toggle button.

- (Optional) Check the required check boxes to enable the corresponding configurations.

Check box	Description
Band Select	Available only when you enable the **2.4 GHz** toggle button.
6 Ghz Client Steering	Available only when you enable the **6 GHz** toggle button.

- From the **Minimum 2.4 GHz Data Rate** and **Minimum 5 GHz Data Rate** drop-down lists, choose the minimum supported data rates for the clients connecting on the band.

  A higher value can improve network performance and reduce interference from legacy devices, but may prevent older and distant clients from connecting. Choose a lower value to maximize compatibility or a higher value to optimize throughput and improve airtime efficiency.

Note Slot availability on APs depends on the AP model. For slots with Flexible Radio Assignment (FRA) capability, FRA can dynamically change the band. This configuration applies to the slot only when it operates in the configured band. Use this configuration to limit WLAN broadcasts by band and slot as needed. Ensure that at least one slot is enabled across the bands.

Step 6 Under **Security**, click **Layer 2** and configure a security policy.

Note WLANs with the same SSID must have unique Layer 2 security policies.

- Click **Enterprise** to configure user credential validation with an 802.1X server for authentication and complete these configurations.

  a. (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

  Use this field if you need a different authorization policy than the global or default list.

  b. (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

  If you do not specify an authorization list in this field, the WLAN uses the default list.

  c. (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

  If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

  To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

  d. (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

  e. Under **WPA Parameters**, check the required check boxes to configure the corresponding settings.

  - **WPA**: configure WPA support.

Note If you check the **WPA3** or **OSEN Policy** check box, this check box is dimmed.

- **WPA2**: configure WPA2 support.
- **WPA3**: configure WPA3 support.

Note If you check the **WPA**, **GTK Randomize**, or **OSEN Policy** check box, this check box is dimmed.

If you enable WPA3, you can optionally check these check boxes to configure the corresponding settings.

- **Transition Disable**: prevent the transition from WPA3 to WPA2.
- **Beacon Protection**: enable beacon protection.

- **GTK Randomize**: enable randomized group temporal key (GTK) for hole 196 mitigation.

  Hole 196 is the name of a WPA2 vulnerability.

Note If you check the **WPA3** check box, this check box is dimmed.

- **OSEN Policy**: configure the Online subscription with Encryption (OSEN) support.

Note If you check the **WPA** or **WPA3** check box, this check box is dimmed.

f. If the **WPA Encryption** area is displayed, check the required check boxes to enable the corresponding cipher support for WPA.

You must enable support for at least one cipher.

g. If the **WPA2/WPA3 Encryption** area is displayed, complete these configurations.

- For wireless controllers running releases earlier than Cisco IOS XE Release 17.15, choose the required encryption type.
- For wireless controllers running Cisco IOS XE Release 17.15 or later, check the check box next to the required encryption types.

h. If the **Auth Key Management** area is displayed, check the required check boxes to choose the corresponding authentication key management types.

The types available under this area vary based on the WPA, WPA2, or WPA 3 encryption settings.

If you check the **CCKM** check box, in the **CCKM TSF Tolerance** field, enter the CCKM tolerance level in milliseconds.

The valid range for this field is from 1000 to 5000. The default value is 1000. Authenticated client devices can roam from one AP to another AP without any perceptible delay during reassociation.

i. Under **Protected Management Frame (802.11w)**, from the **Status** drop-down list, choose an available status.

If you chose **Optional** or **Required**, complete these configurations.

- In the **SA Query Time(msec)** field, enter the Security Association (SA) query retry timeout in milliseconds.

  The valid range is from 100 to 500. The default value is 200.

- In the **Association Comeback Timer(sec)** field, enter the association comeback time in seconds.

  The valid range is from 1 to 20. The default value is 1.

j. Under **Fast Transition (802.11r)**, from the **Fast Transition Mode** drop-down list, choose an available mode.

If you chose **Enabled** or **Adaptive Enabled**, complete these configurations.

- Check the **Over the DS** check box to enable fast transitions over a distributed system.
- In the **Reassociation Timeout** field, enter the reassociation timeout in seconds.

  The valid range is from 1 to 100. The default value is 20.

- Click **Personal** to configure user credential validation using password (PSK with WPA2 encryption) and complete these configurations.

a. (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

Use this field if you need a different authorization policy than the global or default list.

b. (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

If you do not specify an authorization list in this field, the WLAN uses the default list.

c. (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

d. (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

e. Under **WPA Parameters**, check the required check boxes to configure the corresponding settings.

- **WPA**: configure WPA support.

Note If you check the **WPA3** check box, this check box is dimmed.

- **WPA2**: configure WPA2 support.
- **WPA3**: configure WPA3 support.

Note If you check the **WPA** or **GTK Randomize** check box, this check box is dimmed.

If you enable WPA3, you can optionally check the required check boxes to enable the corresponding configurations.

- **Transition Disable**: prevent the transition from WPA3 to WPA2.
- **Beacon Protection**: enable beacon protection.

- **GTK Randomize**: enable randomized GTK for hole 196 mitigation.

  Hole 196 is the name of a WPA2 vulnerability.

Note If you check the **WPA3** check box, this check box is dimmed.

f. If the **WPA Encryption** area is displayed, check the required check boxes to enable the corresponding cipher support for WPA.

You must enable support for at least one cipher.

g. If the **WPA2/WPA3 Encryption** area is displayed, check the **AES(CCMP128)** check box to choose this encryption type.

h. If the **Auth Key Management** area is displayed, check the required check boxes to choose the corresponding authentication key management type.

The options available under this area vary based on the WPA, WPA2, or WPA 3 encryption settings.

Based on the options that you chose, if additional configurations are available, complete these configurations.

- (Optional) From the **PSK Format** drop-down list, choose an authentication preshared key (PSK) format.
- (Optional) From the **PSK Type** drop-down list, choose **Unencrypted**.
- In the **Pre-shared Key** field, enter a PSK value.

  For hexadecimal key format, the PSK length must be 64 characters. For ASCII key format, the PSK length must be in the range 8–63.
- In the **Anti Clogging Threshold** field, enter the Simultaneous Authentication of Equals (SAE) anticlogging threshold.

  The valid range is from 0 to 3000. The default value is 1500.
- In the **Max Retries** field, enter the maximum number of SAE retransmissions.

  The valid range is from 1 to 10. The default value is 5.
- In the **Retransmit Timeout** field, enter the SAE retransmission timeout.

  The valid range is from 1 to 10000. The default value is 400.
- (Optional) From the **SAE Password Element** drop-down list, choose an SAE password element mode.

i. Under **Protected Management Frame (802.11w)**, from the **Status** drop-down list, choose an available status.

If you chose **Optional** or **Required**, enter data in these fields.

- **Association Comeback Timer(sec)**: enter the association comeback time in seconds.

  The valid range is from 1 to 20. The default value is 1.

- **SA Query Time(msec)**: enter the Security Association (SA) query retry timeout in milliseconds.

  The valid range is from 100 to 500. The default value is 200.

j. Under **Fast Transition (802.11r)**, from the **Fast Transition Mode** drop-down list, choose an available mode.

If you chose **Enabled** or **Adaptive Enabled**, complete these configurations.

- Check the **Over the DS** check box to enable fast transitions over a distributed system.
- In the **Reassociation Timeout** field, enter the reassociation timeout in seconds.

  The valid range is from 1 to 100. The default value is 20.

k. (Optional) Under **MPSK**, check the **Enable MPSK** check box to configure multi-preshared key (MPSK) support, and complete these configurations.

Note MPSK and Easy-PSK can't be enabled simultaneously.

If you want to...	Then...
add an MPSK **Note** You can add up to five MPSKs.	**1.** Click **Add**. **2.** In the **Priority** field of the **Add MPSK Configuration** dialog box, enter a priority. The valid range is from 0 to 4. **3.** (Optional) From the **Key Format** drop-down list, choose a format. **4.** (Optional) From the **Password Type** drop-down list, choose **Unencrypted**. **5.** (Optional) In the **Pre-Shared Key** field, enter an MPSK key. **6.** Click **Save**.
edit an MPSK	**1.** Check the check box next to the MPSK that you want to edit. **2.** Hover your cursor over **Actions** and choose **Edit**. **3.** Edit the required configurations. **4.** Click **Save**.

If you want to...	Then...
delete MPSKs	1. Check the check box next to the MPSKs that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

- Click **Static WEP** to configure user credential validation with an 802.1X server for authentication using static Wired Equivalent Privacy (WEP) and complete these configurations.

Note These configurations are unavailable for wireless controllers running Cisco IOS XE Release 26.1.1 or later.

a. (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

Use this field if you need a different authorization policy than the global or default list.

b. (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

If you do not specify an authorization list in this field, the WLAN uses the default list.

c. (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

d. (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

e. Under **Static WEP Parameters**, complete these configurations.

- From the **Key Size** drop-down list, choose a key size.
- In the **Key Index** field, enter the WEP key index to indicate the key that should be used for static WEP authentication.

  The valid range is from 1 to 4.
- From the **Key Format** drop-down list, choose a WEP key format.
- From the **WEP Key Type** drop-down list, choose a WEP key encryption type.
- In the **Wep Key** field, enter a static WEP key.

  The key length depends on the key size that you chose from the **Key Size** drop-down list.

f. (Optional) Under **Fast Transition**, check the **Static WEP Fast Transition** check box to enable fast transition.

- Click **Open Secured** to configure user credential validation using open secured authentication and complete these configurations.

a. (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

   Use this field if you need a different authorization policy than the global or default list.

b. (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

   If you do not specify an authorization list in this field, the WLAN uses the default list.

c. (Optional) Check the **Mac Filtering** check box to enable MAC-based access control or security on the wireless network.

   If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

   To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

d. (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.

e. Check the **WPA3** check box to configure WPA3 support.

f. Under **WPA2/WPA3 Encryption**, check the **AES(CCMP128)** check box to choose this encryption type.

g. Under **Auth Key Management**, check the required check boxes to choose the corresponding authentication key management types.

   The options available under this area vary based on the WPA3 encryption settings.

   If you checked the **OWE** check box, in the **Transition Mode WLAN ID** field, enter the Opportunistic Wireless Encryption (OWE) transition mode WLAN ID.

   The valid range for this WLAN ID is from 0 to 4096. The default value is 0.

h. Under **Protected Management Frame (802.11w)**, from the **Status** drop-down list, choose an available status.

   If you chose **Optional** or **Required**, complete these configurations.

   - In the **Association Comeback Timer(sec)** field, enter the association comeback time in seconds.

     The valid range is from 1 to 20. The default value is 1.

   - In the **SA Query Time(msec)** field, enter the Security Association (SA) query retry timeout in milliseconds.

     The valid range is from 100 to 500. The default value is 200.

- Click **Open** to configure open authentication, and check the required check boxes to enable the corresponding configurations.

  - (Optional) In the **MAC Override Authorization List** field, enter the name of the MAC address authorization list to override the default list for the WLAN.

    Use this field if you need a different authorization policy than the global or default list.

  - (Optional) In the **WLAN Authorization List** field, enter the name of the authorization list to be used for the WLAN.

    If you do not specify an authorization list in this field, the WLAN uses the default list.

  - (Optional) **Mac Filtering**: enable MAC-based access control or security on the wireless network.

    If you check this check box, from the **MAC Authorization List** drop-down list, choose an authorization list.

To create an authorization list, refer to Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

- (Optional) Check the **Lobby Admin Access** check box to enable access to the lobby ambassador account.
- (Optional) **OWE Transition Mode**: configure OWE transition mode.

  If you check this check box, in the **Transition Mode WLAN ID** field, enter the OWE transition mode WLAN ID.

  The valid range for this WLAN ID is from 0 to 4096. The default value is 0.

Step 7 (Optional) Under **Security**, click **Layer 3** and complete these configurations.

a) Check the **Web Policy** check box to configure the web authentication policy.

b) From these drop-down lists, choose the required options.

- **Web Auth Parameter Map**: choose a parameter map for web authentication. To create a web authentication parameter map, refer to Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 809.
- **Authentication List**: choose an authentication list.

  To create an authentication list, refer to Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776.

c) Check the required check boxes to enable the corresponding configurations.

- **On MAC Filter Failure**: enable web authentication on MAC filter failure.
- **Splash Web Redirect**: set a splash-page web redirect

d) (Optional) In the **Web Authorization List** field, enter the name of the web authentication authorization list for the WLAN.

This list permits or denies client access during web authentication sessions.

e) Under **Preauthentication ACL**, choose an IPv4 ACL and IPv6 ACL from the corresponding drop-down lists.

To create an IPv4 ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785. To create an IPv6 ACL, refer to Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792.

Step 8 (Optional) Under **Security**, click **AAA** and complete these configurations.

a) From the **Authentication List** drop-down list, choose an authentication list.

To create a **dot1x** type authentication list, refer to Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776.

b) Check the **Local EAP Authentication** check box to enable the local Extensible Authentication Protocol (EAP) on a WLAN.

If you check this check box, from the **EAP Profile Name** drop-down list, choose a local EAP profile. To create a local EAP profile, refer to Create a local EAP profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 799.

Step 9 (Optional) Under **Advanced**, click **11be** and choose an 802.11be profile for the WLAN.

To create an 802.11be profile, refer to Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 712.

Step 10 (Optional) Under **Advanced**, click **11ax** and complete these configurations.

a) Check the required check boxes to enable the corresponding configurations.

- **Enable 11ax**: enable the 802.11ax configuration.
- **Downlink MU-MIMO**: enable the 802.11ax multiuser MIMO (MU-MIMO) downlink configuration.
- **Downlink OFDMA**: enable the 802.11ax Orthogonal Frequency Division Multiplexing (OFDMA) downlink configuration.
- **Uplink MU-MIMO**: enable the 802.11ax MU-MIMO uplink configuration.
- **Uplink OFDMA**: enable the 802.11ax OFDMA uplink configuration.
- **BSS Target Wake Up Time**: enable 802.11ax target wake-up time support.
- **HE BSS Color Enable**: enable the 802.11ax basic service set (BSS) color configuration.

  If you check this check box, in the **HE BSS Color** field, enter a BSS color value.

  The valid range is from 0 to 255. The default value is 0.
- **HE TWT Enable**: enable 802.11ax target wake-up time.
- **BSS Target Wake Up Time Broadcast**: enable 802.11ax target wake-up time broadcast support.

Step 11 (Optional) Under **Advanced**, click **11k** and complete these configurations.

a) Under **Assisted Roaming**, check the required check boxes to indicate the appropriate status for the corresponding configurations.

- **Prediction Optimization**: indicates if 11k assisted roaming prediction optimization is enabled on the wireless controller for the WLAN.
- **Neighbor List**: indicates if the 11k neighbor list is enabled on the wireless controller for the WLAN.
- **Dual Band Neighbor List**: indicates if the 11k dual-band neighbor list is enabled on the wireless controller for the WLAN.

b) Under **Beacon Radio Measurement**, check the required check boxes to configure the corresponding settings.

- **Client Scan Report on Association**: send a beacon measurement request after client association.
- **Client Scan Report on Roam**: send a beacon measurement request on client roaming.

Step 12 (Optional) Under **Advanced**, click **11v BSS** and complete these configurations.

a) Check the required check boxes to configure the corresponding settings.

- **BSS Transition**: enable BSS transition per WLAN.
- **BSS Max Idle Protected**: enable protected mode for BSS maximum idle processing per WLAN.
- **Dual Neighbor List**: determine if the dual-band neighbor list is enabled in 802.11v BSS transition for WLAN.
- **Directed Multicast Service**: configure Directed Multicast Service (DMS) processing per WLAN.

- **BSS Max Idle Service**: enable BSS maximum idle processing per WLAN.
- **802.11v Disassociate Imminent**: enable BSS transition disassociation imminent per WLAN.
- **802.11v TFS**: enable TFS processing per WLAN.
- **802.11v WNM Sleep Mode**: enable Wireless Network Management (WNM) sleep mode per WLAN.

b) In the **802.11v Disassociate Timer** field, enter the 802.11v disassociation imminent timer in seconds.

The valid range is from 0 to 3000. The default value is 200.

c) In the **802.11v Disassociate Timer Optimized Roaming** field, enter the 802.11v disassociation imminent optimized-roaming timer in seconds.

The valid range is from 0 to 40. The default value is 40.

Step 13 (Optional) Under **Advanced**, click **Device Analytics** and check the required check boxes to enable the corresponding configurations.

- **Advertise Support**: enable device analytics support.
- **Share Data with Client**: enable sharing the Cisco device data with the client.
- **Advertise PC Analytics Support**: enable PC analytics support.

Step 14 (Optional) Under **Advanced**, click **Max Clients** and enter data in these fields.

- **Per WLAN**: enter the maximum number of client connections per WLAN.

  The valid range is from 0 to 32000. The default value is 0.

- **Per AP Per WLAN**: enter the maximum number of client connections per AP that can be configured on a WLAN.

  The valid range is from 0 to 1200. The default value is 0.

- **Per AP Radio Per WLAN**: enter the maximum number of client connections per AP radio that can be configured on a WLAN.

  The valid range is from 0 to 500. The default value is 200.

Step 15 Under **Advanced**, click **Off Channel Scan** and complete these configurations.

a) Under **Defer Priority**, check the required check boxes to choose the corresponding RRM off channel scan defer priority values for packets.

b) In the **Scan Defer Time (msec)** field, enter the required scan defer time in milliseconds.

The valid range is from 0 to 60000. The default value is 100.

Step 16 Under **Advanced**, click **Miscellaneous** and complete these configurations.

a) From the **Peer to Peer Blocking** drop-down list, choose a peer-to-peer blocking configuration on the WLAN.

b) Use the required optionsto configure the corresponding settings.

- **Coverage Hole Detection**: enable Coverage Hole Detection (CHD) on the wireless controller
- **Fastlane+ (ASR)**: enable advanced scheduling request handling on a WLAN
- **Aironet IE**: enable the support for Cisco Compatible Extensions option and set the support for Aironet information element (IE) on the WLAN

- **Advertise AP Name**: advertise the AP name status for the WLAN.
- **Deny LAA (RCM) Clients**: deny the client joining with a locally administered address (random MAC address).
- **IP Source Guard**: enable IP Source Guard (IPSG).

  IPSG is a Layer 2 security feature that prevents the wireless controller from forwarding the packets with source IP addresses that are not known to it.
- **Latency Measurements Announcements**: provide latency information about a radio band so that the client can move to a radio band with better latency if the current radio band is overloaded.
- **Multicast Buffer**: configure multicast buffer tuning mode for 802.11a radio for the WLAN.

  If you check this check box, in the **Multicast Buffer Value** field, enter a value.

  The valid range is from 30 to 60.
- **Opportunistic Key Caching (OKC)**: enable opportunistic key caching (OKC).

  OKC allows the wireless client and the WLAN infrastructure to cache only one Pairwise Master Key (PMK) for the lifetime of the client association with this WLAN, even when roaming between multiple APs.
- **Load Balance**: enable load balance on the WLAN.
- **Media Stream Multicast-Direct**: reliable multicast stream delivery for the WLAN.
- **802.11ac MU-MIMO**: configure 802.11ac MU-MIMO on the WLAN.
- **Universal Admin**: allow universal admin mode to be enabled on a 802.1X, WPA, or WPA2-enabled WLAN.
- **MBO**: enable Wi-Fi Alliance Agile Multiband (MBO) support.

  Note For MBO on a WPA2-enabled WLAN, **Protected Management Frame (802.11w)** must be set to **Required** or **Optional**.
- **Wi-Fi to Cellular Steering**: enable Wi-Fi to cellular steering on the WLAN.

  To enable Wi-Fi to cellular steering, you must enable MBO.

c) (Optional) From the **Wi-Fi Direct Client** drop-down list, choose a Wi-Fi direct-related policy on the WLAN.
d) (Optional) Check the required check boxes to configure the corresponding settings.

- **Ignore RSN IE Len**: enable Robust Secure Network Information Element (RSN IE) validation
- **RE Anchor Roam Clients**: configure the reanchor policy for roaming voice clients.
- **Static IP Tunneling**: enable static IP client tunneling support on the WLAN.
- **UAPSD Compliant**: enable Wi-Fi Multimedia (WMM) Unscheduled automatic power save delivery (U-APSD) compliant client support for WLAN

e) Use the **Enable Fine Timing Measurement Responder** toggle button to configure the AP to act as a Fine Timing Measurement (FTM) responder.

   This option is used for location-based services. It allows compatible clients to measure their distance from the AP for precise indoor positioning.

f) Use the **Advertise AP Location** toggle button to broadcast the physical location of the AP in beacon and probe response frames.

Clients and location-based services can use this information to improve device positioning and navigation accuracy.

g) From the **WMM Policy** drop-down list, choose an option for the policy.

h) From the **mDNS Mode** drop-down list, choose an mDNS operational mode.

i) Under **DTIM Period (in Beacon Intervals)**, in the **5 GHz Band** and **2.4 GHz Band** fields, enter the corresponding Delivery Traffic Indication Map (DTIM) periods.

The valid range is from 1 to 255. The default value is 1. These fields represent the DTIM configuration per WLAN for each 802.11 network.

Step 17 Click **Review and Provision**.

Step 18 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 19 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 20 On the **Tasks** window, monitor the task deployment.

Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a policy profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **SSID** and click **Policy Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create Policy Profile** slide-in pane, complete the required configurations.

a) In the **Policy Profile Name** field, enter a unique name for the policy profile.

The policy profile name can contain up to 32 characters. Catalyst Center does not allow leading or trailing spaces in the policy profile name.

b) (Optional) In the **Description** field, enter a description.
c) Use the toggle buttons to enable or disable the required configurations.

Toggle button	Description
Status	To enable or disable the policy profile.
IP MAC Binding	To configure control over support for IP-MAC address binding creation.
Passive Client	To enable or disable passive client support on a policy.
Encrypted Traffic Analytics	To enable the Encrypted Traffic Analytics feature on the WLAN.

d) Under **WLAN Switching Policy**, enable or disable the required configurations using the toggle buttons.

- **Central Switching**
- **Central DHCP** (for locally switched clients)
- **Central Authentication**
- **Flex NAT/PAT**

Note Local switching, central DHCP, and IPv4 DHCP required must be enabled before enabling this option.

e) (Optional) Under **CTS Policy**, configure the required Cisco TrustSec (CTS) policies.

- Check the **Inline Tagging** check box to enable inline tagging for clients.
- Check the **SGACL Enforcement** check box to enable Security Group ACL (SGACL) enforcement of CTS policies on the device.
- In the **Default SGT** field, enter a default Security Group Tag (SGT) value.

  The valid range is from 2 to 65519. The default value is 2.

Step 6 (Optional) Click **Access Policies** and configure the required access policies.

a) Check the required check boxes to enable the corresponding configurations.

b) Under **WLAN Local Profiling**, in the **Local Subscriber Policy Name** field, enter the name of a policy map.

To create a policy map, refer to Create a policy map for a Cisco Catalyst 9800 Series Wireless Controller, on page 908.

c) Under **VLAN**, complete the required configurations.

- In the **VLAN/VLAN Group** field, enter the text to search for a VLAN or VLAN group. From the drop-down list, choose a VLAN or VLAN group.
- In the **Multicast VLAN** field, enter the multicast VLAN ID associated with the WLAN.

  The valid range is from 1 to 4094.
- In the **OSEN Encryption VLAN** field, enter VLAN ID to be used for OSEN encrypted traffic on this WLAN.

  This VLAN can contain up to 8 characters.

d) Under **WLAN ACL**, complete these configurations:

- From the **IPv4 ACL** drop-down list, choose an IPv4 ACL.

  To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785.
- From the **IPv6 ACL** drop-down list, choose an IPv6 ACL.

  To create an ACL, refer to Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792.
- In the **Layer 2 ACL** field, enter the name of the Layer 2 ACL for the WLAN.

e) Under **URL Filters**, choose the pre-authentication and post-authentication URL filters from the corresponding drop-down lists.

Note We recommend that you use enhanced URL filters for only FlexConnect local switching deployments.

To create URL filters, refer to Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 803 and Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 804.

Step 7 Click **QoS and AVC** and complete the required configurations.

a) From the **Auto QoS** drop-down list, choose an auto-QoS mode for the WLAN.

b) (Optional) In the **Re-anchor Classmap Name** field, enter the name of the classmap containing the protocols for selective reanchoring.

c) (Optional) Check the **NBAR Protocol Discovery** check box to enable Network-Based Application Recognition (NBAR) protocol discovery for the WLAN.

d) (Optional) Check the **QBSS Load** check box to advertise QoS-enhanced BSS load IE.

e) (Optional) If you chose the auto-QoS mode **None**, under **QoS SSID Policy** and **QoS Client Policy**, choose QoS SSID policy names from the **Egress** and **Ingress** drop-down lists.

To create a QoS policy, refer to Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 910.

f) Under **Flow Monitor IPv4** and **Flow Monitor IPv6**, choose flow monitors from the **Egress** and **Ingress** drop-down lists.

To create a flow monitor, refer to Create a flow monitor for a Cisco Catalyst 9800 Series Wireless Controller, on page 916.

Step 8 Under **SIP-CAC**, check the required check boxes to enable the corresponding configurations.

Check box	Description
Call Snooping	To enable call snoop for the WLAN mapped to the policy profile **Note** When you enable call snoop, you must configure Platinum SSID policies.
Send 486 Busy	To enable SIP CAC to send 486 busy
Send Disassociate	To enable SIP CAC send disassociate

Step 9 (Optional) Click **Mobility** and configure mobility anchors.

a) Under **Mobility Anchors**, complete the required configurations.

- Check the **Export Anchor** check box to indicate that the WLAN mapped to the policy is an anchor WLAN.

Note When you enable this option, central switching is enabled. You must disable the Link Local Bridging feature.

- Check the **Static IP Mobility** check box to enable static IP mobility.

Note You can't enable static IP mobility and mobility anchor simultaneously.

b) Under **Anchors**, add or remove mobility anchors.

Note This action causes the WLANs that are enabled to be momentarily disabled resulting in loss of connectivity for some clients.

If you want to...	Then...
add an anchor	1. Click **Add**. 2. In the **Add** dialog box • From the **Anchor IP** drop-down list, choose a mobility anchor IP. • From the **Anchor Priority** drop-down list, choose a priority for the mobility anchor. 3. Click **Save**.
edit an anchor	1. Check the check box next to the anchor IP. 2. Hover your cursor over **Actions** and choose **Edit**. 3. Edit the required configuration. 4. Click **Save**.
delete an anchor	1. Check the check box next to the anchor IP. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

Step 10 Click **WLAN Scheduler** and configure a scheduler for WLAN.

If you want to...	Then...
add a WLAN scheduler	a. Click **Add**. b. In the **Add Wlan Scheduler** dialog box • From the **Calendar Profile Name** drop-down list, choose a calendar profile. • Use the **Client Session Disable** toggle button to enable or disable client session based on the calendar profile. • Use the **Wlan Enable** toggle button to enable or disable the policy profile based on the calendar profile. c. Click **Save**.
edit a WLAN scheduler	a. Check the check box next to the WLAN scheduler. b. Hover your cursor over **Actions** and choose **Edit**. c. Edit the required configuration. d. Click **Save**.

If you want to...	Then...
delete WLAN scheduler	**a.** Check the check box next to the WLAN scheduler. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 11 Under **Advanced**, click **WLAN Timeout** and configure the client WLAN timeout.

a) In the **Session Timeout (sec)** field, enter the client session timeout in seconds.

The valid range is from 0 to 86400. The default value is 28800.

b) In the **Idle Timeout (sec)** field, enter the duration of an idle timeout in seconds.

The valid range is from 15 to 100000. The default value is 300.

c) In the **Idle Threshold (bytes)** field, enter the idle threshold in bytes.

The default value is 0.

d) In the **Client Exclusion Timeout** field, enter the client exclusion timeout value.

The valid range is from 0 to 2147483647. The default value is 60.

e) (Optional) Check the **Guest LAN Session Timeout** check box to enable session timeout for guest LAN.

f) (Optional) Check the **Client Exclusion** check box to enable client exclusion for the WLAN.

Step 12 (Optional) Under **Advanced**, click **WLAN Flex Policy** and configure a WLAN flex policy.

a) Check the **VLAN Central Switching** check box to configure VLAN central switching.

Note VLAN-based central switching isn't supported when AAA override is disabled.

b) In the **Split MAC ACL** field, enter the split MAC ACL name.

To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785.

Step 13 (Optional) Under **Advanced**, click **AAA Policy** and configure the AAA policy.

a) Check the **AAA Override** check box to enable AAA override.

b) If you enable AAA override, use the **NAC State** check box to enable or disable Network Admission Control (NAC).

If you check this check box, from the **NAC Type** drop-down list, choose an option.

c) Check the **VLAN Fallback** check box to enable fallback to policy profile VLAN when override VLAN is unavailable.

d) From the **AAA Policy Name** drop-down list, choose an AAA policy.

To create an AAA policy, refer to Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 784.

e) From the **Accounting List** drop-down list, choose an accounting list.

To create an accounting list, refer to Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 778.

f) Check the **Interim Accounting** check box to enable interim accounting messages.

Step 14 (Optional) Under **Advanced**, click **DHCP** and configure DHCP for wireless clients.

a) Check the **IPv4 DHCP Required** check box to enforce DHCP for all the clients on the WLAN.

Note This option must be enabled before enabling the **Flex NAT/PAT** option.

b) In the **DHCP Server IP Address** field, enter an IPv4 DHCP server for the WLAN.

c) From the **DHCP Server VRF** drop-down list, choose the VRF name for the IPv4 DHCP server.

To create a VRF interface, refer to Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

d) Use the **Disable DHCP Option** toggle button to enable or disable inclusion of additional DHCP options in DHCP requests for this WLAN.

e) Use the **DHCPv6 Relay Option VPN** toggle button to enable or disable the association of DHCPv6 relay options with a VPN context for the WLAN policy.

f) In the **DHCPv6 Server Address** field, enter the IPv6 address of the IPv6 DHCP server to which the client requests are relayed for the WLAN policy.

Enter a valid IPv6 address that is reachable from the wireless controller. This IPv6 address is required for networks using external IPv6 DHCP servers.

g) From the **DHCPv6 Server VRF Name** drop-down list, choose a VRF name.

To create a VRF interface, refer to Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

h) Check the required check boxes to enable the corresponding DHCP Option 82 configurations.

Step 15 (Optional) Under **Advanced**, click **DNS Layer Security** and configure DNS layer security.

a) In the **DNS Layer Security Parameter Map** field, enter a map name.

To create an accounting list, refer to Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 778.

b) From the **Flex DNS Traffic Redirect** drop-down list, choose an umbrella DNA traffic redirect option.

c) Check the **Flex DHCP Option for DNS** check box to enable the DNS DHCP option.

Step 16 (Optional) Under **Advanced**, click **Miscellaneous** and configure miscellaneous wireless profile configurations such as user-defined (private) network, air time fairness, and so on.

a) In the **mDNS Service Policy** field, enter a name for the service policy.

The service policy name can contain up to 64 characters. To create a service policy, refer to Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 890.

b) From the **Hotspot Server** drop-down list, choose a server.

c) Check the required check boxes to enable the corresponding configurations.

- **Link Local Bridging**: enable link-local bridging

Note You must disable the WLAN mobility policy anchor when link-local bridging is enabled.

- **Multicast Filter**: enable the filter to drop all multicast downstream packets
- **Rate None**: enable the client Address Resolution Protocol (ARP) rate limiting

d) In the **Burst Interval** field, enter the burst interval in seconds.

The valid range is from 3 to 255. The default value is 5.

e) In the **Rate Pps** field, enter a value for the allowed ARP packet rate.

The valid range is from 15 to 1500. The default value is 100.

f) Use the **L3 Access** toggle button to enable or disable Layer 3 access.

g) Under **User Defined (Private) Network**, check the required check boxes to enable the corresponding configurations.

- **Status**: enable user-defined (private) network
- **Drop Unicast**: set the action to drop the user-defined (private) network unicast traffic

h) Under **Air Time Fairness Policies**, from the **2.4 GHz Policy** and **5 GHz Policy** drop-down lists, choose a corresponding policy.

i) Under **WGB Parameters**, complete the required configurations.

- Check the **Broadcast Tagging** check box to enable workgroup bridge (WGB) broadcast tagging
- Check the **WGB VLAN** check box to enable client VLAN support
- Use the **Multicast Forwarding for Foreign APs** toggle button to enable or disable multicast traffic forwarding for clients connected to foreign APs in guest or mobility scenarios.

j) Under **Policy Proxy Settings**, complete the required configurations.

- Check the **ARP Proxy** check box to enable the ARP proxy feature.
- From the **IPv6 Proxy** drop-down list, choose an IPv6 Neighbor Discovery (ND) proxy feature.

k) Under **EoGRE Tunnel Profile**, from the **Tunnel Profile** drop-down list, choose a tunnel profile.

To create a tunnel profile, refer to Create an EoGRE tunnel profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 920.

Step 17 Click **Review and Provision**.

Step 18 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).

Option	Description
Cancel	Close the dialog box.

Step 19 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 20 On the **Tasks** window, monitor the task deployment.

Create a remote LAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a remote LAN (RLAN) profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **SSID** and click **Remote LAN Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create Remote LAN Profile** slide-in pane, complete these configurations.

a) In the **RLAN Profile Name** field, enter a unique name for the RLAN profile.

Note Ensure that the RLAN profile name does not match any existing WLAN profile names. Otherwise, the RLAN profile creation task fails.

b) In the **RLAN ID** field, enter an RLAN profile ID.

The valid range is from 1 to 128. The default value is 1.

c) Use the **Status** toggle button to enable or disable the RLAN profile.
d) (Optional) In the **Client Association Limit** field, enter a value for the maximum number of client connections per RLAN. The default value is 0.
e) From the **mDNS Mode** drop-down list, choose a mode on RLAN.

Step 6 Under **Security**, click **Layer 2** and configure Layer 2 security policies for the RLAN.

a) (Optional) Check the **802.1X** check box to enable 802.1X.

b) (Optional) From the **MAC Filtering** drop-down list, choose an option.

To create an authorization list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

c) (Optional) From the **Authentication List** drop-down list, choose an authentication list of type DOT1x.

To create an authentication list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776.

d) From the **Fallback Mechanism** drop-down list, choose an RLAN fallback authentication type.

e) (Optional) Check the **EAP-Identity-Request Retries Status** check box to enable the EAP identity request retry settings.

- In the **EAP-Identity-Request Max Retries** field, enter the maximum number of EAP identity request retransmissions.

  The valid range is from 1 to 20.

- In the **EAP-Identity-Request Timeout (sec)** field, enter a timeout value for the EAP identity requests in seconds.

  The valid range is from 1 to 120.

f) (Optional) Check the **EAP-Request Retries Status** check box to enable the EAP request retry settings.

- In the **EAP-Request Max Retries** field, enter the maximum number of EAP request retransmissions.

  The valid range is from 1 to 20.

- In the **EAP-Request Timeout (sec)** field, enter a timeout value for the EAP requests in seconds.

  The valid range is from 1 to 120.

Step 7 (Optional) Under **Security**, click **Layer 3** and configure the Layer 3 policies and ACL for the RLAN.

a) Check the **Web Auth** check box to enable security web authentication.

Note You can't enable web authentication and 802.1X simultaneously.

b) From the **Web Auth Parameter Map** drop-down list, choose a map.

To create a web authentication profile, see Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 809.

Associating an RLAN profile with web authentication provides user authentication through a web portal, which enhances security and provides better access control over the wireless network.

c) From the **Authentication List** drop-down list, choose an authentication list of the type login.

To create an authentication list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776.

d) Under **Preauthentication ACL**, choose the required ACL from the corresponding drop-down list.

- **IPv4** (to create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785)
- **IPv6** (to create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792)

Step 8 (Optional) Under **Security**, click **AAA** and check the **Local EAP Authentication** check box to enable an EAP profile on an RLAN.

If you check this check box, from the **EAP Profile Name** drop-down list, choose an EAP profile name.

Associating an RLAN profile with local EAP enhances security, access control, compliance, network performance, user management, troubleshooting, and scalability in a wireless network environment.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create a remote LAN policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a remote LAN (RLAN) policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **SSID** and click **Remote LAN Policies**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create Remote LAN Policy** slide-in pane, complete the required configurations.

a) In the **RLAN Policy Name** field, enter a name for the RLAN policy.

The RLAN policy name can contain up to 32 characters.

b) (Optional) In the **Description** field, enter a description.
c) Use the **Status** toggle button to enable or disable the RLAN policy.
d) (Optional) Check the **PoE** check box to enable Point over Ethernet (PoE).
e) From the **Power Level** drop-down list, choose a power level for the AP PoE port.
f) Under **RLAN Switching Policy**, use the **Central Switching** and **Central DHCP** toggle buttons to enable or disable the corresponding configurations.

Step 6 Click **Access Policies** and complete the required configurations.

a) (Optional) Check the **Pre-Authentication** check box to enable pre-authentication.
b) (Optional) From the **VLAN** drop-down list, enter the text to search for a VLAN. From the drop-down list, choose a VLAN.

To create a VLAN, see Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 934.

c) From the **Host Mode** drop-down list, choose a host mode for the RLAN.
d) (Optional) Under **RLAN ACL**, choose an IPv4 ACL and IPv6 ACL from the drop-down lists.

- **IPv4 ACL** (to create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785)
- **IPv6 ACL** (to create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792)

Step 7 Click **Advanced** and complete the required configurations.

a) From the **Violation Mode** drop-down list, choose a violation mode for the RLAN.
b) (Optional) In the **Session Timeout (sec)** field, enter a value for the session timeout in seconds.

The valid range is from 0 to 86400. The default value is 28800.



Note To disable the session timeout, enter 0.

c) (Optional) From the **mDNS Service Policy** drop-down list, choose an mDNS service policy name.

To create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 890.

d) (Optional) Under **User Defined (Private) Network**, check the required check boxes to enable the corresponding configurations.

- **Status**: enable user-defined (private) network
- **Drop Unicast**: set the action to drop the user-defined (private) network unicast traffic

e) (Optional) Under **AAA Policy**, complete the required configurations.

- Check the **AAA Override** check box to enable AAA override.
- From the **AAA Policy Name** drop-down list, choose an AAA policy.

  To create an AAA policy, see Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 784.
- From the **Accounting List** drop-down list, choose an accounting list.

  To create an accounting list, see Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 778.

f) (Optional) Under **Split Tunnel**, complete the required configurations.

- Check the **Status** check box to enable a split tunnel.
- From the **ACL** drop-down list, choose an ACL.

  To create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785.

g) (Optional) Under **Exclusionlist**, complete the required configurations.

- Uncheck the **Status** check box to disable the client exclusion.
- In the **Exclusionlist Timeout** field, enter the time for which the client is excluded.

  The valid range is from 0 to 2147483647. The default value is 60.

h) (Optional) Under **DHCP**, complete the required configurations.

- Check the **IPv4 DHCP Required** check box to enforce DHCP for all the clients on the remote LAN.
- In the **DHCP Server IP Address** field, enter an IPv4 DHCP server for the remote LAN.
- From the **DHCP Server VRF** drop-down list, choose an IPv4 DHCP server VRF name for the remote LAN.

i) Under **Miscellaneous**, check the required check boxes to enable the corresponding configurations.

Check box	Description
ARP Rate None	To enable the client Address Resolution Protocol (ARP) rate limiting. If you check this check box, complete these configurations. • In the **ARP Rate PPS** field, enter a value for the allowed ARP packet rate. The valid range is from 15 to 1500. The default value is 100. • In the **ARP Burst Interval** field, enter the burst interval in seconds. The valid range is from 3 to 255. The default value is 5.
NDP Rate None	To enable the client Neighbor Discovery Protocol (NDP) rate limiting. If you check this check box, complete these configurations. • In the **NDP Rate PPS** field, enter a value for the allowed NDP packet rate. The valid range is from 15 to 1500. The default value is 100. • In the **NDP Burst Interval** field, enter the burst interval in seconds. The valid range is from 3 to 255. The default value is 5.

Step 8 Click **Review and Provision**.

Step 9 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create a policy tag for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a policy tag for the APs associated with a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **SSID** and click **Policy Tags**.

Step 4 Click **Add**.

Step 5 In the **Tag Name** field of the **Create Policy Tags** slide-in pane, enter a unique name for the policy tag.

Step 6 (Optional) In the **Description** field, enter a description.

Step 7 (Optional) Under **WLAN Profile - Policy Profile Mapping**, configure the WLAN profile to policy profile mapping.

If you want to...	Then...
add a WLAN profile to policy profile mapping	**a.** Click **Add**. **b.** From the **WLAN Profile** drop-down list, choose a WLAN profile. **c.** From the **Policy Profile** drop-down list, choose a policy profile. **d.** Click **Save**.
edit a WLAN profile to policy profile mapping	**a.** Check the check box next to the required WLAN profile name. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete WLAN profile to policy profile mappings	**a.** Check the check box next to the required WLAN profile names. **b.** Hover your cursor over **Actions** and choose **Delete** **c.** In the dialog box, click **Yes**.

Step 8 (Optional) Under **RLAN Profile - RLAN Policy Mapping**, configure RLAN profile to RLAN policy mapping.

If you want to...	Then...
add an RLAN profile to RLAN policy mapping	**a.** Click **Add**. **b.** From the **Port ID** drop-down list, choose the RLAN port ID value of the AP. **c.** From the **RLAN Profile** drop-down list, choose an RLAN profile. **d.** From the **RLAN Policy Profile** drop-down list, choose an RLAN policy profile. **e.** Click **Save**.
edit an RLAN profile to RLAN policy mapping	**a.** Check the check box next to the required port ID. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete RLAN profile to RLAN policy mappings	**a.** Check the check box next to the required port IDs. **b.** Hover your cursor over **Actions** and choose **Delete** **c.** In the dialog box, click **Yes**.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Configure the 802.11be profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure or create an 802.11be profile for a wireless controller and provision it. 802.11be profile is applicable for wireless controllers that are running Cisco IOS XE Release 17.15.1 or later.

Wireless controllers that are running versions earlier than Cisco IOS XE Release 17.18.1 use a single 802.11be profile, which is the default-dot11be-profile. Wireless controllers that are running Cisco IOS XE Release 17.18.1 or later support custom 802.11be profiles.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **SSID** and click **802.11be Profiles**.

Step 4 Complete one of these applicable configurations:

If you want to...	Then...
configure 802.11be profile for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1	**a.** Click the radio button next to the default 802.11be profile. **b.** Hover your cursor over **Actions** and click **Edit**.
create 802.11be profile for a wireless controller running Cisco IOS XE Release 17.18.1 or later	click **Add**.

Step 5 In the **Profile Name** field, enter a unique name for the 802.11be profile for a wireless controller running Cisco IOS XE Release 17.18.1 or later.

The profile name can contain up to 32 characters. Catalyst Center does not support leading and trailing spaces in the profile name.

Step 6 (Optional) In the **Description** field, update the description.

The description can contain up to 64 characters,

Step 7 (Optional) Use the available toggle buttons to enable or disable the corresponding parameters.

- **Downlink OFDMA**: enables downlink connection to use OFDMA for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.

- **Uplink OFDMA**: enables uplink connection to use OFDMA for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **Downlink MU-MIMO**: enables downlink connection to use MU-MIMO for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **Uplink MU-MIMO**: enables uplink connection to use MU-MIMO for a wireless controller running a version earlier than Cisco IOS XE Release 17.18.1.
- **OFDMA Multi-RU**: enables the assignment of multiple Resource Units (RUs) simultaneously to a single user using OFDMA.

Note To configure OFDMA and MU-MIMO for a wireless controller running Cisco IOS XE Release 17.18.1 or later, use the **Advanced** > **11ax** tab in the WLAN profile. For more information, see Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 683.

Step 8 (Optional) Use the toggle buttons to enable or disable these MLO group configurations for a wireless controller running Cisco IOS XE Release 17.18.1 or later:

- **Primary 2.4GHz**: configures the 2.4-GHz band in the MLO group
- **Primary 5GHz**: configures the 5-GHz band in the MLO group
- **Secondary 5GHz**: configures a secondary 5-GHz band in the MLO group
- **Primary 6GHz**: configures the 6-GHz band in the MLO group

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

RF configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device RF configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an RF profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **RF** and click **RF Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create RF Profiles** slide-in pane, configure the required parameters.

a) In the **RF Profile Name** field, enter a unique name for the RF profile.

The profile name can contain up to 32 characters. Catalyst Center does not allow the ? character in the profile name.

b) (Optional) In the **Description** field, enter a description.
c) From the **Radio Band** drop-down list, choose a radio band for the RF profile.

If you chose **6 GHz**, you can optionally allow the AP to operate in the standard power mode. Check the **Allow Standard Power Mode** check box to enable standard power mode.

d) Use the **Status** toggle button to enable or disable the RF profile.
e) From the **NDP Mode** drop-down list, choose an operating mode.

Step 6 Click **802.11** and do these steps:

a) Under **Operational Data Rates**, choose the required configuration for the corresponding data rates from the drop-down lists.
b) For the 5-GHz and 2.4-GHz bands, under **802.11n MCS Rates**, check the check box for the required Modulation Coding Scheme (MCS) index.

Step 7 Under **RRM**, click **Trap Thresholds** and complete the required configurations.

a) In the **Interference (%)** field, enter an interference threshold in percent.

The valid range is from 0 to 100. The default value is 10.

When the interference exceeds this threshold, traps are generated.

b) In the **Clients** field, enter a threshold for the number of clients per AP radio to trigger a trap.

The valid range is from 1 to 200. The default value is 12.

c) In the **Noise (dBm)** field, enter the noise threshold in dBm.

The valid range is from -127 to 0. The default value is -70.

d) In the **Utilization (%)** field, enter a threshold for the bandwidth used by an AP in percent.

The valid range is from 0 to 100. The default value is 80.

Step 8 Under **RRM**, click **Coverage** and complete the required configurations.

a) In the **Minimum Client Level (clients)** field, enter the minimum client exception level.

The valid range is from 1 to 200. The default value is 3.

b) In the **Data RSSI Threshold (dBm)** field, enter the Received Signal Strength Indicator (RSSI) threshold value for data packets in dBm.

The valid range is from -90 to -60. The default value is -80.

c) In the **Voice RSSI Threshold (dBm)** field, enter the RSSI threshold value for voice packets in dBm.

The valid range is from -90 to -60. The default value is -80.

d) In the **Exception Level (%)** field, enter the coverage exception level in percent.

The valid range is from 1 to 100. The default value is 25.

Step 9 Under **RRM**, click **TPC** and complete the required configurations.

a) In the **Maximum Power Level (dBm)** field, enter the upper limit of the transmit power in dBm.

The valid range is from -10 to 30. The default value is 30.

For 802.11 networks, this configuration is accepted only when Transmit Power Control (TPC) is in Auto or Run Once mode.

b) In the **Minimum Power Level (dBm)** field, enter the lower limit of the transmit power in dBm.

The valid range is from -10 to 30. The default value is -10.

For 802.11 networks, this configuration is accepted only when TPC is in Auto or Run Once mode.

c) In the **Power Control Threshold (dBm)** field, enter the TPC version 1 threshold for RRM in dBm.

The valid range is from -80 to -50. The default value is -70.

d) In the **Tx Power V2 Threshold** field, enter the TPC version 2 threshold for RRM in dBm.

The valid range is from -80 to -50. The default value is -67.

Step 10 Under **RRM**, click **DCA** and complete the required configurations.

a) (Optional) Check the **Avoid AP Foreign AP Interference** check box to configure Dynamic Channel Assignment (DCA) for RF profiles.

If you configure DCA, the device RRM algorithms consider 802.11 traffic from foreign APs that aren't included in your wireless network when assigning channels.

b) Under **DCA Channels**, check the check box for the required channel numbers.
c) (Optional) Check the **Zero Wait DFS** check box to enable the 802.11a Zero Wait DFS feature.

Note This feature is applicable for only the 5-GHz band.

d) From the **Channel Width** drop-down list, choose a DCA channel width for the RF profile.

Note This drop-down list is available for only the 6-GHz and 5-GHz bands.

e) If you chose the 5-GHz or 6-GHz band, choose the minimum and maximum channel width allowed for DBS from the **Channel Width Min** and **Channel Width Max** drop-down lists.
f) (Optional) Check the **PSC Enforcement** check box to enable Preferred Channel Scanning (PSC) for the 6-GHz DCA.
g) Under **High Speed Roam**, complete these configurations.

- For the 2.4-GHz and 5-GHz bands, complete these configurations:
  - (Optional) check the **Mode Enable** check box to configure high-speed roam (HSR) mode for the RF profile, and
  - In the **Neighbor Timeout** field, enter the timeout interval of the neighbors for the RF profile.

    The valid range is from 5 to 60. The default value is 5.

- From the **Client Network Preference** drop-down list, choose a client network preference.
  - **Connectivity**: the RRM algorithm uses connectivity of the clients as network preference.
  - **Throughput (Bps)**: the RRM algorithm uses the high throughput of the clients as network preference.
  - **Default**: the RRM algorithm doesn't use any network preferences.

Step 11 If you chose the 2.4-GHz band, under **RRM**, click **Band Select** and complete these configurations.

a) (Optional) Check the **Band Select Probe Response** check box to enable the 802.11ax broadcast probe response.
b) In the **Client RSSI (dBm)** field, enter the minimum mobile station RSSI threshold in dBm.

The valid range is from -90 to -20. The default value is -80.

c) In the **Client Mid-RSSI (dBm)** field, enter the medium mobile station RSSI threshold in dBm.

The valid range is from -90 to -20. The default value is -80.

d) In the **Cycle Count (cycles)** field, enter the number of suppression cycles for a new client.

The valid range is from 1 to 10. The default value is 2.

e) In the **Cycle Threshold (msec)** field, enter the scan cycle threshold for band select in milliseconds.

The valid range is from 1 to 1000. The default value is 200.

f) In the **Expire Dual Band (sec)** field, enter the expiration time for dual band in seconds.

The valid range is from 10 to 300. The default value is 60.

g) In the **Expire Suppression (sec)** field, enter the expiration time of suppression in seconds.

The valid range is from 10 to 200. The default value is 20.

Step 12 Click **802.11ax** and complete the required configurations.

a) If you chose the 6-GHz band, complete these configurations.

- From the **6 GHz Discovery Frames** drop-down list, choose a discovery frame for the 802.11ax 6-GHz band.
- In the **He Bcast Probe Resp Intvl** field, enter an 802.11ax broadcast probe response interval.

  The valid range is from 5 to 25. The default value is 20.
- From the **Multi BSSID Profile** drop-down list, choose a multi-BSSID profile.

  To create a multi-BSSID profile, refer to Create a multi-BSSID profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 724.

b) Under **Spatial Reuse**, complete the required configurations.

- (Optional) Check the **OBSS PD** check box to enable Overlapping BSS Packet Detect (OBSS-PD) spatial reuse.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold in dBm.

  The valid range is from -82 to -62. The default value is -62.
- (Optional) Check the **SRG OBSS PD** check box to enable SRG OBSS-PD spatial reuse.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold in dBm.

  The valid range is from -82 to -62. The default value is -82.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold in dBm.

  The valid range is from -82 o -62. The default value is -62.

Step 13 Click **Advanced** and complete the required configurations.

a) (Optional) In the **A-MPDU Window Size** field, enter Aggregated MAC Protocol Data Unit (A-MPDU) window size.

The valid range is from 1 to 255. The default value is 255.

b) Under **High Density Parameters**, complete the required configurations.

- In the **Max Clients** field, enter the maximum number of clients per AP in a high-density environment.

  The valid range is from 0 to 500. The default value is 200.
- From the **Multicast Data Rate (Mbps)** drop-down list, choose a minimum data rate at which the multicast clients can associate with AP.

Note The value 0 indicates that the AP automatically adjusts the data rates.

- From the **Rx SOP Threshold (dBm)** drop-down list, choose a Receiver Start of Packet Detection (RX SOP) sensitivity threshold in dBm.

  If you chose the **Custom** RX SOP threshold, the **RX-SOP Threshold (dBm) Custom Value** field is displayed. In this field, enter a custom value for the RX SOP threshold in dBm. The value range is from -85 to -60.

c) Under **Client Distribution**, complete the required configurations.

- In the **Load Balancing Window** field, enter the number of clients to load balance across APs.

  The valid range is from 0 to 20. The default value is 5.

- In the **Load Balancing Denial Count** field, enter the load balance denial count for APs.

  The valid range is from 1 to 10. The default value is 3.

d) Under **ATF Configuration**, complete the required configurations.

From the **ATF Optimization** drop-down list, choose an option to enable or disable airtime fairness for the RF profile. When airtime fairness optimization is enabled, the wireless controller dynamically reallocates airtime from underutilized clients to the clients that need more bandwidth. This optimization improves network efficiency.

For the 5-GHz and 2.4-GHz bands, complete these configurations:

- From the **Status** drop-down list, configure the airtime fairness operating mode.
- Check the **Bridge Client Access** check box to enable the air time allocation mode on the default RF policy.

  If you check this check box, in the **Airtime Allocation** field, you can optionally enter an air time allocation weight percentage.

  The valid range is from 5 to 90. The default value is 5.

e) Under **FRA**, complete the required configurations.

Band	Action
6 GHz	• In the **Client Reset Count** field, enter the client-aware FRA client count for dual-band radios to switch from the 6-GHz to 5-GHz band. The valid range is from 1 to 10. The default value is 1. • In the **Client utilization threshold (%)** field, enter the client-aware FRA utilization threshold value for dual-band radios to switch from the 6-GHz to 5-GHz band.

Band	Action
5 GHz	Use the **Client Aware** check box to enable or disable client-aware FRA. Client-aware FRA allows the dual-band radios to operate in 5-GHz or monitor mode depending on the load on the dedicated 5-GHz band. If you check this check box, enter data in these fields: • **Client Select**: enter the client-aware FRA utilization threshold value for dual-band radios to switch from monitor mode to client-serving mode. The valid range is from 0 to 100. The default value is 50. • **Client Select**: enter the client-aware FRA utilization threshold value for dual-band radios to switch from client-serving mode to monitor mode. The valid range is from 0 to 100. The default value is 5.
2.4 GHz	From the **FRA Action** drop-down list, choose an FRA action for dual-band radios.

f) Under **RSSI Settings**, complete the required configurations.

- (Optional) Check the **RSSI Low Check** check box to indicate if the RSSI low check is enabled before enabling the optimized roaming feature.
- In the **RSSI Threshold (dBm)** field, enter the minimum RSSI threshold for optimized roaming.

  The valid range is from -127 to 0. The default value is -127.

g) Under **UNII Band Settings**, use the **UNII-3 Low Power Channels** check box to enable or disable the use of UNII-3 low power channels within the 5-GHz band for the RF profile.

When enabled, APs can use these channels to potentially reduce interference and improve the network performance.

Note This check box is not applicable to the 6-GHz and 2.4-GHz bands.

h) (Optional) Under **Retry Limits**, enter data in these fields:

- **Aggregate Retries**: enter the maximum number of retransmission attempts for aggregated data frames before dropping them.

  The valid range is from -1 to 255. The default value is -1.
- **Management Retries**: enter the maximum number of retransmission attempts for management frames before dropping them.

  The valid range is from -1 to 255. The default value is -1.
- **Non-Aggregate Retries**: enter the maximum number of retransmission attempts for non-aggregated data frames before dropping them.

  The valid range is from -1 to 255. The default value is -1.

Step 14 Click **802.11be** and use the **Preamble Puncture** toggle button to enable or disable preamble puncturing.

Preamble puncturing improves spectral efficiency by excluding portions of channels with interference while maintaining wider bandwidths.

Note This tab is not available for the 2.4-GHz band.

Step 15 Click **Review and Provision**.

Step 16 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 17 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 18 On the **Tasks** window, monitor the task deployment.

Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a radio antenna profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **RF** and click **Radio Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create Radio Profile** slide-in pane, complete these configurations:

a) In the **Radio Profile Name** field, enter a unique name for the radio antenna profile.

The profile name can contain up to 32 characters. Catalyst Center does not support leading and trailing spaces in the profile name.

b) (Optional) In the **Description** field, enter a description.

c) From the **Antenna Beam** drop-down list, choose a beam steering mode for the AP slot.

d) (Optional) In the **Number of Antennas to be Enabled** field, enter the number of antennas to be enabled for the AP slot.

The valid range is from 0 to 8.

e) (Optional) Check the required check boxes to enable the corresponding configurations.

Check box	Description
Mesh Backhaul	To enable mesh backhaul on this radio.
Mesh Designated Downlink	To use this radio as a designated mesh downlink backhaul. If a designated downlink backhaul is available, the uplink radio isn't used as a downlink radio.

f) From the **Wireless Active Testing Radio Administrative State** drop-down list, choose the required state.

If you choose **Enabled (Always)**, the radio is always available to be selected for Wireless Active Testing (WAT).

g) Under **DTIM Period**, in the **6 GHz Band** field, enter a Delivery Traffic Indication Map (DTIM) interval for the 6-GHz band.

The valid range is from 1 to 255. The default value is 1.

Step 6 In the **URWB** tab, from the **URWB Radio Role** drop-down list, choose a radio role.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).

Option	Description
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an RF tag for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an RF tag for the APs associated with a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **RF** and click **RF Tags**.

Step 4 Click **Add**.

Step 5 In the **Tag Name** field of the **Create RF Tag** slide-in pane, enter a unique name for the RF tag.

The name can contain up to 32 characters.

Step 6 (Optional) In the **Description** field, enter a description.

Step 7 (Optional) From these drop-down lists, choose the required RF profile for the corresponding band.

- **6 GHz RF Profile** (to create a 6-GHz RF profile, see Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 714)
- **5 GHz RF Profile** (to create a 5-GHz RF profile, see Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 714)
- **2.4 GHz RF Profile** (to create a 2.4-GHz RF profile, see Create an RF profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 714)

Step 8 From the **AP Beam State** drop-down list, choose the beamforming state of the AP.

Step 9 (Optional) Click **Show Slot Configuration** to view and update the slot configurations.

From these drop-down lists, choose the required radio antenna profile for the corresponding band and slot.

- **6 GHz Slot 2 Radio Profile**
- **6 GHz Slot 3 Radio Profile**
- **6 GHz Slot 1 Radio Profile**
- **5 GHz Slot 1 Radio Profile**
- **5 GHz Slot 2 Radio Profile**
- **5 GHz Slot 0 Radio Profile**
- **2.4 GHz Slot 0 Radio Profile**
- **2.4 GHz Slot 2 Radio Profile**

To create a radio antenna profile, refer to Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 720.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create a multi-BSSID profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a multi-basic service set identifier (BSSID) profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **RF** and click **Multi BSSID Profiles**.

Step 4 Click **Add**.

Step 5 In the **Multi BSSID Profile Name** field of the **Create Multi BSSID Profile** slide-in pane, enter a name for the multi-BSSID profile.

Step 6 (Optional) In the **Description** field, enter a description.

Step 7 (Optional) Under **802.11ax**, use the available check boxes to enable the corresponding parameters.

Step 8 (Optional) Under **802.11be**, use the available check boxes to enable the corresponding parameters.



Note For a wireless controller running Cisco IOS XE Release 17.18.1 or later, use the **Downlink OFDMA**, **Uplink OFDMA**, **Downlink MU-MIMO**, and **Uplink MU-MIMO** check boxes under **802.11ax** in Step 7, on page 724 to configure the corresponding parameters.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create a URWB network profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Ultra Reliable Wireless Backhaul (URWB) network profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the URWB network profile configuration page.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.
d) Click the device name.
e) In the dialog box with the device information, click **View Device Details** to open the device details window.
f) In the **Configuration** tab, expand **RF** and click **URWB Network Profile**.

Step 2 Click **Add**. In the **General** tab of the **Create URWB Network Profile** slide-in pane, configure the settings as described:

a) Click the **URWB Status** toggle button to enable the URWB feature.
b) In the **URWB Network Profile Name** field, enter a unique name for the URWB network profile.
c) (Optional) In the **Description** field, enter a description.
d) Check the **Strong Network Key** check box to configure a strong password evaluation for the network key.
e) Select **Unencrypted** or **AES** from the **Network Key Type** drop-down list.
f) In the **Network Key** field, enter the URWB network key.

The network key must be between 8 and 63 characters long. Additionally, the network key must include at least one uppercase letter, one lowercase letter, and at least one digit or special character.

Step 3 In the **Mobility** tab of the **Create URWB Network Profile** slide-in pane, configure these settings:

a) In the **Mobility Role** drop-down list, select **Base**, **Base Relay**, or **Client** for the Backhaul device.
b) In the **Traffic Egress Point** field, select the coordinator or the wireless controller for mobility traffic.
c) Configure these **Mobility Backhaul Check** parameters:

1. **Ethernet Down**: Configure handoff when all ethernet ports are disconnected.
2. **Coordinator Down**: Configure handoff when coordinator is unreachable.

d) Configure these **Mobility Scan** parameters:

1. **Isolation**: Enter the timeout value to trigger an active scan when the device is disconnected from the infrastructure.
2. **Periodic**: Enter the time interval to perform periodic background channel scanning while the device is idle.
3. **RSSI Threshold**: Enter the RSSI threshold value to trigger scanning when the received signal strength falls below this level.

Step 4 In the **MPO** tab, configure the **Packet Duplication Mode**.

Step 5 In the **Advanced** tab, complete these configurations:

a) In the **Ethernet Protocols** area, choose **None**, **All**, or a specific protocol from the **Allow Ether Types** drop-down list.

To allow only custom Ether values, select **List** from the **Allow Ether Types** drop-down list.

b) Check the **Legacy Ethernet** check box to allow Ethernet I frames forwarding.
c) In the **Unicast** area, check the **Unicast Flood** check box to enable unicast flood and enter unicast flood limitation.
d) Check the **Unicast Flood Limitation** check box to flood one packet every 5 seconds
e) Select the **Multicast** option from the drop-down list.
f) In the **High Availability** area, check the **High Availability Enabled** check box.
g) In the **High Availability Timeout** field, enter the timeout value.

Step 6 In the **Wired Ports** tab, complete these configurations:

a) (Optional) In the **Ethernet Settings area**, select the port associated with the URWB network profile from the **Secondary LAN Port** drop-down list.
b) Check the **LAN Port PoE** check box to specify whether Power over Ethernet is configured for the secondary LAN port associated with this profile.

Only the C9124AXI, C9124AXE, and C9124AXD models support LAN Port PoE.

c) In the **Local Authentication** area, choose the server from the **RADIUS Server Group** drop-down list to be used for authentication, authorization and accounting in this wireless profile.

This option is disabled if the mobility role is not client. To create a RADIUS server group, refer to Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 770.

d) In the **NAT** area, complete these configurations:

1. **Enable NAT**: Check this check box to configure NAT settings for the URWB profile.
2. **NAT Address**: Enter the public IP address to be used for NAT. This address will be presented to external networks for client traffic originating from this wireless profile.
3. **Netmask**: Enter the subnet mask for the NAT IP address. This defines the network range for NAT operations and should match your network's addressing scheme.
4. **Outside Port Range**: Enter the starting port number and ending port number for the range of outbound NAT ports.
5. **NAT Rules:** Click **Add** to create NAT rules using these parameters:

- **Protocol**: Choose the TDP or UDP protocol from the drop-down list.
- **Outside Port**: Enter a port number between 1 and 65535.
- **Inside IP**: Enter a valid IPv4 address.

- **Inside Port**: Enter a port number between 1 and 65535.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Edit default RF settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to edit the default RF settings for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **RF** and click **RF Defaults**.

Step 4 Select the required band. Hover your cursor over **Actions** and choose **Edit**.

Alternatively, click the required band.

Step 5 In the **Edit RF Defaults** slide-in pane, under **Roaming & Client Settings**, complete these configurations:

- In the **Maximum Clients per Radio** field, enter the maximum number of clients allowed to connect to each radio on APs that use this band.

  The valid range is from 0 to 500.

- From the **Client Network Preference** drop-down list, choose the preferred network behavior for clients associated with this band.
  - **Connectivity Optimized**: Prioritize stable connection.
  - **Throughput Optimized**: Maximize data rates.
  - **Default (Controller Decision)**: Use the default settings on the wireless controller.

Step 6 (Optional) For the default 5-GHz RF profile, under **Channel Width Settings**, select the minimum and maximum channel width allowed for dynamic bandwidth selection from the corresponding drop-down lists.

Note The minimum channel width must be less than or equal to the maximum channel width.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

AP configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device AP configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP join profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **AP Join Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create AP Join Profile** slide-in pane, complete these configurations.

a) In the **AP Join Profile Name** field, enter a unique name for the AP join profile.

AP join profile name can contain up to 32 characters. Catalyst Center does not allow leading and trailing spaces in the AP join profile name.

b) (Optional) In the **Description** field, enter a description.
c) From the **Country Code** drop-down list, choose a country code for the AP.



Important As required by the End-User License Agreement (EULA), choose an appropriate country code to ensure that the network complies with local and national regulatory restrictions. Improper country code assignment can disrupt wireless transmissions and result in government-imposed penalties and sanctions on wireless network operators using devices with incorrect country codes.

d) From the **Time Zone** drop-down list, choose an option for the time zone.

If you chose **Delta From WLC**, in the **Offset** area, enter data in these fields.

- **HH**: enter an offset hour for time zone.

  The valid range is from -12 to 14. The default value is 0.

- **MM**: enter an offset minute for time zone.

  The valid range is from 0 to 59. The default value is 0.

e) From the **Deployment Mode** drop-down list, choose an AP deployment mode.



Note Changing the deployment mode may cause the AP to rejoin and result in loss of connectivity for the associated clients.

f) Check the required check boxes to enable the corresponding configurations.

- **LED State**: enable the LED status
- **USB Enable**: enable USB
- **LAG Mode**: enable the AP LAG mode
- **Apphost**: enable IOX application hosting

g) (Optional) In the **NTP Server** field, enter a valid NTP server IP address.
h) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Fallback to DHCP**: enable AP fallback to DHCP

  When this check box is checked, if the AP fails to join through the static IP address, the AP falls back to the DHCP.

- **GAS AP Rate Limit**: enable the Generic Advertisement Services (GAS) rate limit on the AP

  If you check this check box, enter data in these fields.

  - **GAS Request limit interval (msec)**: enter the interval to define the GAS request rate limit in milliseconds.

    The valid range is from 100 to 10000.

  - **Maximum Allowed GAS/ANQP Requests**: enter the maximum number of GAS requests allowed per AP slot in an interval.

The valid range is from 1 to 100.

i) (Optional) Enter data in these fields.

- **NTP Server Info Key**: enter a key ID that identifies the NTP authentication key.

  The valid range is from 1 to 65535. The default value is 1.

- **NTP Server Trust Key**: enter the trust key to use in NTP authentication.

j) From the **NTP Server Key type** drop-down list, choose the encryption to use when storing the trust key locally.

k) (Optional) In the **Led Flash (sec)** field, enter the LED flash timer duration for AP in seconds.

The valid range is from 0 to 3600. The default value is 0.

l) (Optional) Check the **DHCP Server Enable** check box to enable the DHCP server.

m) (Optional) In the **Fast Channel** field, enter a value for the fast channel mode number.

The valid range is from 0 to 4294967295.

n) Under **OfficeExtend AP Configuration**, check the required check boxes to enable the corresponding configurations.

- **Local Access**: enable local access on Office Extended AP (OEAP)
- **Rogue Detection**: enable rogue detection on OEAP
- **Link Encryption**: enable data encryption on OEAP
- **Provisioning SSID**: enable provisional SSID on OEAP

o) Under **Antenna Monitoring**, complete these configurations.

- (Optional) Check the **Antenna Monitoring** check box to enable antenna monitoring.
- In the **RSSI Fail Threshold (dB)** field, enter the RSSI failure threshold value for antenna monitoring in dB.

  The valid range is from 10 to 90. The default value is 40.

- In the **Weak RSSI (dBm)** field, enter the weak RSSI value for antenna monitoring.

  The valid range is from -90 to -10. The default value is -60.

- In the **Detection Time (min)** field, enter the detection time for antenna monitoring.

  The valid range is from 9 to 180. The default value is 12.

Step 6 Click **Client** and complete these configurations.

a) In the **Maximum Client Limit** field, enter the maximum number of clients per AP configuration.

The valid range is from 0 to 1200. The default value is 0.

b) In the **Statistics Timer (sec)** field, enter the time in seconds that the AP sends its 802.11 statistics to the wireless controller.

c) (Optional) Check the **RSSI Client Statistics** check box to enable client RSSI statistics reporting from AP.

d) (Optional) In the **RSSI Statistics Interval** field, enter the reporting interval for the client RSSI statistics from AP to wireless controller.

The valid range is from 30 to 300. The default value is 30.

e) Under **TCP MSS Configuration**, complete these configurations.

- (Optional) Use the **Enable Adjust MSS** check box to enable or disable the TCP MSS adjustment.
- In the **Adjust MSS** field, enter the global AP TCP MSS value.

  The valid range is from 536 to 1363. The default value is 1250.

Step 7 Under **CAPWAP**, click **High Availability** and complete these configurations.

a) Under **CAPWAP Timers**, enter data in these fields.

- **Fast Heartbeat Timeout (sec)**: enter a timeout value for the heartbeat timer for all APs in seconds.

  The valid range is from 0 to 10. The default value is 0.
- **Heartbeat Timeout (sec)**: enter a timeout value for the heartbeat timer for AP discovery in seconds.

  The valid range is from 0 to 30. The default value is 30.
- **Discovery Timeout (sec)**: enter a timeout value for the AP discovery in seconds.

  The valid range is from 1 to 10. The default value is 10.
- **Primary Discovery Timeout (sec)**: enter a timeout value for the primary AP discovery in seconds.

  The valid range is from 30 to 3000. The default value is 120.
- **Primed Join Timeout (sec)**: enter a primed timeout value for AP discovery in seconds.

  The valid range is from 0 to 43200. The default value is 0.

b) Under **Retransmit Timers**, enter data in these fields.

- **Count**: enter the retransmit timer count.

  The valid range is from 3 to 8. The default value is 5.
- **Interval (sec)**: enter the retransmit timer interval in seconds.

  The valid range is from 2 to 5. The default value is 3.

c) Under **AP Fallback to Primary Controller**, use the **Enable** check box to enable or disable fallback to backup controllers.

Fallback applies to the primary controller and doesn't apply to the backup primary controller.

d) (Optional) Under **Backup Primary Controller** and **Backup Secondary Controller**, enter data in these fields.

- **Name**: enter the controller name for the AP
- **IPv4/IPv6 Address**: enter the IP address of the controller for the AP

Step 8 Under **CAPWAP**, click **Advanced** and complete these configurations.

a) Check the required check boxes to enable the corresponding configurations.

Enable Data Encryption: enable data encryption for the AP

- **Enable Jumbo MTU**: enable Jumbo MTU for the AP

b) From the **Link Latency** drop-down list, choose a link auditing option.

c) From the **Preferred Mode** drop-down list, choose a preferred mode for CAPWAP.
d) In the **CAPWAP Window Size** field, enter a CAPWAP window size for request packets in a multiwindow queue.

The valid range is from 1 to 50. The default value is 1.

e) Under **Discovery**, complete these configurations:

- Use the **Private** check box to enable or disable discovery response from a private IP address.
- Use the **Public** check box to enable or disable discovery response from public IP address.
- From the **Onboarding Configuration** drop-down list, choose the CAPWAP discovery onboarding configuration for AP.

Step 9 Under **AP**, click **General** and complete these configurations.

a) Under **Power Over Ethernet**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Switch Flag**: enable 802.3af switches
  - **Power Injector State**: if a power injector is being used
- From the **Power Injector Type** drop-down list, choose the type of power injector.

  If you chose **Installed** or **Override**, in the **Injector Switch MAC** field, enter the MAC address of the power injector switch.

b) Under **AP EAP Authentication**, complete these configurations.

Under **EAP Type**, choose an authentication method.

- **No-Auth**: default authentication method.
- **EAP-TLS**: EAP-Transport Level Security (EAP-TLS) uses certificate-based authentication.

  If you choose EAP-TLS, enter a username. Catalyst Center generates a certificate and applies it during the PnP claim process.
- **EAP-PEAP**: EAP-Protected Extensible Authentication Protocol (EAP-PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. EAP-PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol.

  If you choose EAP-PEAP, enter a username and password. Catalyst Center generates a certificate and applies it during the PnP claim process.
- **EAP-FAST**: EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

  If you choose EAP-FAST, enter a username and password to be applied during the PnP claim process.

This authentication method is used during the AP PnP claim and day-*n* authentication. Changing the authentication method impacts the service of the APs onboarded through the PnP claim process. If you change the authentication method, perform a factory reset for the APs onboarded through the PnP claim process. If an AP joins with a different

Extensible Authentication Protocol (EAP) method, the EAP method changes based on the authentication method that you choose.

From the **AP Authorization Type** drop-down list, choose a Locally Significant Certificates (LSC) AP authorization type.

c) Under **Client Statistics Reporting Interval**, enter a report interval (in seconds) at which the AP sends client statistics for all the clients connected to the corresponding band in the **5 GHz (sec)** and **2.4 GHz (sec)** fields.

The valid range is from 5 to 90. The default value is 90.

d) (Optional) Under **Extended Module**, check the **Enable** check box to enable the AP extended module.

e) (Optional) Under **Mesh**, in the **Mesh Profile Name** field, enter a mesh profile name.

To create a mesh profile, see Create a mesh profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 747.

f) (Optional) Under **Interface Settings**, in the **AP Static MTU Size** field, enter the Maximum Transmission Unit (MTU) size for AP.

The valid values are 0 (to disable) or range from 576 and 1485.

g) (Optional) Under **MACsec Encryption**, complete these configurations.

- Check the **Enable MACsec Encryption** check box to enable Media Access Control Security (MACsec) for AP. This option provides Layer 2 encryption, enhancing security on wired connections to protect data in transit between the AP and wireless controller.
- From the **MACsec Pre-shared Key Chain** drop-down list, choose a key chain.

  To create a key chain, see Create a key chain for a Cisco Catalyst 9800 Series Wireless Controller, on page 830.
- In the **MACsec Replay Window Size** field, enter a number to specify the size of the replay protection window for MACsec.

  This value determines how many out-of-order packets are accepted, helping to prevent replay attacks while accommodating some network jitter.
- Check the **Automatic MACsec** check box to enable automatic detection and MACsec establishment between Cisco Catalyst 9350 Switches and Wi-Fi 7 APs that support this feature.

h) (Optional) Under **Advanced AP Features**, check the required check boxes to enable the corresponding configurations.

- **RLAN Fast Switching**: enable or disable fast switching for Remote LAN (RLAN) interfaces. When enabled, APs can switch RLAN traffic efficiently and reduce latency.
- **NSI Ports**: enable or disable the Network Service Interface (NSI) on the AP.

  NSI ports are used for advanced network network services and diagnostics.
- **CAPWAP Packet Aggregation**: enable or disable CAPWAP aggregation for the AP.

  Aggregation improves performance by reducing overhead on CAPWAP tunnels.
- **Accelerometer Sensor**: enable or disable the accelerometer sensor on the AP. When enabled, AP can detect motion or tampering events.

Step 10 (Optional) Under **AP**, click **Power Management** and complete these configurations.

a) Under **Regular Power Profile**, from the **Regular Power Profile** drop-down list, choose a power profile that is applied to APs.

If an AP doesn't receive the required power, it functions in a derated state as defined by the sequence of rules in the power profile.

To create a power profile, see Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 751.

b) Under **Calendar Profile - Power Profile Mapping**, configure power profile mapping.

If you want to...	Then...
add a power profile mapping	1. Click **Add Mapping**. 2. In the **Add Calendar Profile - Power Profile Mapping** dialog box, from the **Calendar Profile** drop-down list, choose a calendar profile. To create a calendar profile, see Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 759. 3. From the **Power Profile** drop-down list, choose a power profile. To create a power profile, see Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 751. 4. Click **Save**.
edit a power profile mapping	1. Check the check box next to the required calendar profile. 2. Hover your cursor over **Actions**, and choose **Edit**. 3. Edit the mapping. 4. Click **Save**.
delete a power profile mapping	1. Check the check box next to the required calendar profile. 2. Hover your cursor over **Actions** and choose **Delete** 3. In the dialog box, click **Yes**.

Step 11 Under **AP**, click **Hyperlocation** and complete these configurations.

a) (Optional) Check the **Enable Hyperlocation** check box to enable hyperlocation.

b) If you uncheck the **Enable Hyperlocation** check box, enter data in these fields.

- **Detection Threshold (dBm)**: enter a value to filter out packets with low RSSI.

  The valid range is from -100 to -50. The default value is -100.

- **Trigger Threshold (cycles)**: enter a value to set the number of scan cycles before sending a BAR to clients.

  The valid range is from 1 to 100. The default value is 10.

- **Reset Threshold**: enter a value to reset the value in scan cycles after the trigger.

  The valid range is from 0 to 99. The default value is 8.

Step 12 Under **AP**, click **AP Statistics** and complete these configurations.

a) Under **System Monitoring**, complete these configurations.

- (Optional) Check the **Monitor Real Time Statistics** check box to enable AP statistics collection and processing.
- (Optional) Check the **Trigger Alarm for AP** check box to enable the AP statistics alarm.
- In the **CPU Threshold to Trigger Alarm (%)** and **Memory Threshold to Trigger Alarm (%)** fields, enter the threshold percentage for CPU and memory usage respectively.

  The valid range is from 0 to 100. The default value is 0.

  An SNMP trap is sent when this threshold is crossed.
- In the **Interval to Hold Alarm (sec)** field, enter the time in seconds for which the alarm is held before it gets triggered.

  The valid range is from 0 to 3600. The default value is 6.
- In the **Trap Retransmission Time (sec)** field, enter the time between retransmissions of the alarm in seconds.

  The valid range is from 0 to 65535. The default value is 0.
- In the **Sampling Interval (sec)** field, enter a value in seconds to define how often the data is collected from the AP.

  The valid range is from 2 to 900. The default value is 30.
- In the **Statistics Interval (sec)** field, enter a value in seconds to define the interval at which AP statistics are calculated.

  The valid range is from 120 to 900. The default value is 300.
- (Optional) Check the **Reload the AP** check box to automatically reload the AP when there's high CPU and memory usage in the defined sampling interval.

b) Under **Radio Monitoring**, complete these configurations.

- (Optional) Check the **Monitoring of AP Radio Stuck** check box to enable AP radio statistics collection and processing.
- (Optional) Check the **Alarms for AP Radio Stuck** check box to generate an alarm for the AP radio when there's no increment in the statistics.
- Check the **Reset the Stuck AP Radio** check box to enable AP radio reset and recover the radio when there's no increment in the statistics.
- In the **Sampling Interval (sec)** field, enter a value in seconds to define how often data is collected from the radio.

  The valid range is from 720 to 3600. The default value is 720.

Step 13 Under **Management**, click **Device** and complete these configurations.

a) (Optional) Under **TFTP Downgrade**, enter data in these fields.

- **IPv4/IPv6 Address**: enter the TFTP downgrade IP address of the TFTP server
- **Image File Name**: enter the name of the TFTP downgrade file

b) Under **System Log**, complete these configurations.

- From the **Facility Value** drop-down list, choose a facility value.
- (Optional) In the **Host IPv4/IPv6 Address** field, enter the IPv4 or IPv6 address of the host.
- From the **Log Trap Value** drop-down list, choose a log level.
- (Optional) Check the **Secured** check box to enable TLS mode for secure syslog.

c) Under **Telnet/SSH**, complete these configurations.

- Use the **Telnet** check box to enable or disable a Telnet session to the AP.
- Use the **SSH** check box to enable or disable an SSH session to the AP.
- Use the **Serial Console** check box to enable or disable access to the serial console to the AP.
- From the **Console Port Speed** drop-down list, choose a baud rate for the AP console port to match your terminal or console server settings for serial access.

d) Under **AP Core Dump**, complete these configurations.

- From the **Kernel Core Dump** drop-down list, choose a type of kernel core dump.



Note Changing the kernel core dump type may cause the AP to rejoin and result in loss of connectivity for the associated clients.

- In the **Max AP Kernel Core Dumps** field, enter the maximum number of kernel core dumps.

  The valid range is from 1 to 5. The default value is 5.

- (Optional) Check the **Radio Core Dump** check box to enable AP core dump.

  If you enable AP core dump, complete these configurations.

  - (Optional) Check the **Enable File Compression** check box to enable file compression.
  - In the **TFTP Server (IPv4/IPv6)** field, enter the TFTP server address to move the core dump.
  - In the **File Name** field, enter a core file name.

- In the **Kernel Coredump File Limit** field, enter the maximum number of core dump files to retain on the AP. When the limit is reached, older files are deleted.

  The valid range is from 15 to 25. The default value is 25.

Step 14 Under **Management**, click **User** and complete these configurations.

- (Optional) In the **Username** field, enter a user name for AP user management.

  You can enter up to 32 characters.

- From the **Password Type** drop-down list, choose a type of password for AP user management.
- (Optional) In the **Password** field, enter a password for AP user management.

- From the **Secret Type** drop-down list, choose a type for secret for AP user management.
- (Optional) In the **Secret** field, enter a secret for AP user management.

Step 15 Under **Management**, click **Credentials** and complete these configurations.

- (Optional) In the **Dot1x Username** field, enter a user name for AP Dot1x authentication.

  You can enter up to 32 characters.
- (Optional) In the **Dot1x Password** field, enter a password for AP Dot1x authentication.
- From the **Dot1x Password Type** drop-down list, choose a type of password for AP Dot1x authentication.

Step 16 (Optional) Under **Management**, click **CDP** and check the **CDP State** check box to enable CDP for the AP.

Step 17 Click **Security** and complete these configurations.

a) Under **Rogue Detection**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Rogue Detection**: detect APs that are installed on a secure network without authorization from the system administrator.
  - **Rogue Containment Automatic Rate Selection**: enable rogue containment automatic rate selection.
  - **Auto Containment on FlexConnect Standalone**: enable rogue containment for FlexConnect mode.
- Enter data in these fields.
  - **Rogue Detection Minimum RSSI**: enter the minimum RSSI for AP rogue detection.

    The valid range is from -128 to -70. The default value is -90.
  - **Rogue Detection Transient Interval (sec)**: enter the transient interval in seconds for which the rogue AP should be seen before reporting the wireless controller.

    The valid values are 0 or range from 120 to 1800. The default value is 0.
  - **Rogue Detection Report Interval (sec)**: enter the interval in seconds at which the monitor mode report is generated for AP rogue detection.

    The valid range is from 10 to 300.

b) (Optional) Under **PMF - Denial**, check the **Rogue Containment PMF-Denial** check box to enable 802.11w Protected Management Frames (PMF) denial rogue AP containment.

If you check this check box, you can optionally use these check boxes to enable or disable the corresponding configurations:

- **Rogue Containment PMF-Deauth**: PMF denial rogue AP containment using deauthentication.
- **Rogue Detection PMF Off-Channel**: off-channel PMF rogue AP containment

c) (Optional) Under **aWIPS and Forensic Capture**, check the **aWIPS** check box to enable the Advanced Wireless Intrusion Prevention System (aWIPS).

If you enable aWIPS, the **Forensic Capture** check box is displayed. To enable aWIPS forensic capture, check the **Forensic Capture** check box.

Step 18 (Optional) Under **iCAP Client Telemetry**, click **Full Packet Trace** and complete these configurations.

a) Check the required check box to enable the corresponding configurations.

- **Topic Status**: enable the full packet trace subscription for Intelligent Capture (iCAP) clients
- **Aggregate Trace**: enable aggregation of full packet traces

b) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

Step 19 (Optional) Under **iCAP Client Telemetry**, click **Partial Packet Trace** and complete the configurations.

a) Check the **Topic Status** check box to enable partial packet trace subscription for iCAP clients.

b) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

To include additional MAC addresses, click the plus icon.

c) Under **Protocol Filters**, complete these configurations.

- Under **Protocol Filter Type**, check the **All** check box to collect partial packet traces for all protocols.
- Under **Management Type**, check the check box next to the required management protocols to collect the partial packet traces: **All**, **Assoc**, and **Auth**
- Under **Data Type**, check the check box next to the required data protocols to collect the partial packet traces: **All**, **ARP**, **DHCP**, **DHCPv6**, **DNS**, **EAP**, **ICMP**, and **ICMPv6**
- Under **Cisco Type**, check the check box next to the required Cisco protocols to collect the partial packet traces: **All** and **NDP**

Step 20 Under **iCAP Client Telemetry**, click **Anomaly Detection** and complete these configurations.

a) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Topic Status**: enable the anomaly detection subscription for iCAP clients
- **Packet Trace Trigger AP**: trigger an AP packet trace on anomaly detection

b) (Optional) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

To include additional MAC addresses, click the plus icon.

c) Under **Timeout**, in the **DHCP Frequency (sec)** field, enter a DHCP timeout for anomaly detection in seconds.

The valid range is from 1 to 120. The default value is 5.

Step 21 Under **iCAP Client Telemetry**, click **Statistics** and complete these configurations.

a) Under **Client Statistics Subscription**, complete these configurations.

- (Optional) Check the **Topic Status** check box to enable client statistics subscription for iCAP clients.
- In the **Frequency (sec)** field, enter the frequency for client statistics collection in seconds.

  The valid range is from 30 to 3600. The default value is 30.

b) Under **Client Filter Statistics Subscription**, complete these configurations.

- (Optional) Check the **Topic Status** check box to enable client statistics subscription for iCAP filtered clients.
- In the **Frequency (sec)** field, enter the frequency for filtered client statistics collection in seconds.

The valid range is from 5 to 3600. The default value is 5.

c) (Optional) Under **Client MAC Filters**, in the **MAC Address** field, enter the MAC address of the client.

To include additional MAC addresses, click the plus icon.

Step 22 Click **iCAP AP Telemetry Subscriptions** and complete these configurations.

a) Check the required check boxes to enable the corresponding configurations.

- **RF Spectrum**: enable iCAP AP telemetry subscription for RF spectrum
- **Slot 0**: use radio slot 0 for RF spectrum measurements
- **Slot 1**: use radio slot 1 for RF spectrum measurements
- **Slot 2**: use radio slot 2 for RF spectrum measurements
- **Slot 3**: use radio slot 3 for RF spectrum measurements

b) (Optional) Configure the statistics subscription.

- Check the required check boxes to enable the corresponding AP statistics subscription.
- In the corresponding **Frequency (sec)** fields, enter a frequency for the corresponding AP statistics collection in seconds.

  The valid range is from 30 to 3600. The default value is 30.

Step 23 (Optional) Click **QoS** and complete these configurations.

a) Use the required check boxes to enable or disable the corresponding configurations.

- **Action Frame**: send an 802.11 QoS map action frame when the DSCP to User Priority (UP) mapping changes
- **Trust DSCP Upstream**: configure the AP to trust the upstream DSCP instead of UP

b) Under **DSCP to UP Range**, configure the DSCP to UP range mapping.

If you want to...	Then...
add a DSCP to UP range mapping	1. Click **Add**. 2. From the **User Priority** drop-down list in the **Add DSCP to UP Range** dialog box, choose a user priority. 3. In the **UP to DSCP Upstream** field, enter an AP upstream traffic UP to DSCP mapping. The valid range is from 0 to 63. The default value is 0. 4. In the **Lower DSCP Range** field, enter a lower boundary for the DSCP range. The valid range is from 0 to 63. The default value is 0. 5. In the **Upper DSCP Range** field, enter an upper boundary for the DSCP range. The valid range is from 0 to 63. The default value is 0. 6. Click **Save**.
edit a DSCP to UP range mapping	1. Check the check box next to the required user priority. 2. Hover your cursor over **Actions** and choose **Edit**. 3. Edit the required configurations. 4. Click **Save**.
delete a DSCP to UP range mapping	1. Check the check box next to the required user priority. 2. Hover your cursor over **Actions**, and choose **Delete**. 3. In the dialog box, click **Yes**.

c) Under **DSCP to UP Exception**, configure the DSCP to UP exception mapping.

If you want to...	Then...
add a DSCP to UP exception mapping	1. Click **Add**. 2. In the **DSCP** field of the **Add DSCP to UP Exception** dialog box, enter DSCP to map to UP. The valid range is from 0 to 63. 3. From the **User Priority** drop-down list, choose a user priority. 4. Click **Save**.

If you want to...	Then...
edit a DSCP to UP exception mapping	1. Check the check box next to the required DSCP. 2. Hover your cursor over **Actions** and choose **Edit**. 3. Edit the required configurations. 4. Click **Save**.
delete DSCP to UP exception mapping	1. Check the check box next to the required DSCP. 2. Hover your cursor over **Actions**, and choose **Delete**. 3. In the dialog box, click **Yes**.

Step 24 Click **Geolocation** and configure the required settings.

Under **Fine Timing Measurement**, complete these configurations:

- Use the **FTM Enabled** check box to enable or disable Fine Timing Measurement (FTM).
- From the **FTM Initiator Burst Duration** drop-down list, choose a duration.
- In the **FTM Initiator Burst Size** field, enter the FTM initiator burst size.

  The valid range is from 2 to 31. The default value is 16.

Under **Ultra-Wide Band (UWB)**, complete these configurations:

- Use the **UWB** check box to enable or disable Ultra-Wide Band (UWB) for AP location tracking.
- In the **UWB Burst Duration** field, enter the UWB burst duration for optimized AP location tracking.

  The valid range is from 5 to 30. The default value is 10.
- In the **UWB Burst Size** field, enter the UWB burst size for optimized AP location tracking.

  The valid range is from 10 to 100. The default value is 32.
- Use the **UWB Wi-Fi Blocking** check box to enable or disable the blocking of Wi-Fi transmissions during Ultra-Wide Band (UWB) operations.

  Enable this setting to reduce interference between UWB and Wi-Fi, which may be necessary for certain location-based services.

  If you check this check box, from the **UWB Wi-Fi Block Duration** drop-down list, choose a duration for which Wi-Fi is blocked during UWB operations on the AP.

  Longer durations may improve UWB accuracy but can temporarily impact Wi-Fi connectivity.

Step 25 Click **Miscellaneous** and complete these configurations.

- (Optional) In the **Packet Capture Profile** field, enter a name for the packet capture profile.
- (Optional) In the **AP Trace Profile** field, choose an AP trace profile.
- (Optional) In the **Beacon Power** field, enter a Bluetooth Low Energy (BLE) beacon power value.

  The valid range is from 40 to 100. The default value is 59.

- (Optional) In the **Beacon Interval** field, enter a BLE beacon interval for the AP.

  The valid range is from 1 to 10. The default value is 1.

- (Optional) Check the **SSID Statistics Enable** check box to enable BSSID statistics on an AP.

  Note You can't enable BSSID statistics and client traffic distribution status on an AP simultaneously.

- (Optional) In the **SSID Profile Statistics Frequency** field, enter the time frequency on AP to send BSSID statistics.

  The valid range is from 1 to 180. The default value is 30.

- (Optional) Check the **SSID Neighbor Statistics Enable** check box to enable BSSID neighbor statistics on AP.

- (Optional) In the **SSID Neighbor Statistics Frequency** field, enter the time interval between consecutive BSSID neighbor statistics update sent from the AP.

  The valid range is from 0 to 180. The default value is 180.

- (Optional) Use the **ICAP Individual Enable** check box to enable the anomaly detection report for individual anomalies.

- (Optional) In the **ICAP Individual Throttle** field, enter the number of events per five minutes for anomaly detection individual reports.

  The valid range is from 0 to 500. The default value is 5.

- (Optional) Check the **ICAP Summary Enable** check box to enable the anomaly detection report summary.

- (Optional) In the **ICAP Summary Frequency** field, enter a frequency for anomaly detection summary reports.

  The valid range is from 3 to 60. The default value is 5.

- (Optional) Check the **Partial Trace Management Probe** check box to collect partial packet traces for probing management protocols.

- (Optional) In the **AUX LAN ID** field, enter the VLAN ID to which auxiliary client traffic is assigned.

  The valid range is from 0 to 4094. The default value is 0.

- From the **Press Sense Config State** drop-down list, choose an AP pressure sensor configuration state.

- (Optional) In the **Proxy Hostname** field, enter the HTTP proxy host name.

- (Optional) In the **Proxy List** field, enter a list of URLs to exclude from the proxy.

- (Optional) In the **Proxy Port** field, enter the HTTP proxy port number.

  The valid range is from 0 to 65535.

- (Optional) From the **Accounting Method List** field, choose an accounting method list name.

  To create an accounting method list, see Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 778.

- (Optional) In the **AP Management IPv4 ACL Name** field, enter the name of the IPv4 ACL to restrict management access to the AP.

The ACL name can contain up to 32 characters. Only the devices permitted in this ACL can manage the AP over IPv4.

- (Optional) In the **AP Management IPv6 ACL Name** field, enter the name of the IPv6 ACL to restrict management access to the AP.

  The ACL name can contain up to 32 characters. Only the devices permitted in this ACL can manage the AP over IPv6.

- (Optional) Check the **Traffic Distribution Status** check box to enable client traffic distribution statistics.

  Note You can't enable BSSID statistics and client traffic distribution status on an AP simultaneously.

- (Optional) In the **Traffic Distribution Interval** field, enter an interval at which the AP sends the statistics.

  The valid range is from 30 to 3600. The default value is 300.

- (Optional) In the **Session Limit** field, enter the maximum Dot1x sessions allowed per AP.

  The default value is 0.

- From the **Tunnel UDP Lite** drop-down list, choose an IPv6 CAPWAP data checksum type.

- (Optional) Check the required check boxes to enable or disable the corresponding configurations.

  - **GPRC Enable**: enable gRPC server on the AP, check the check box
  - **TLS Config Control Preference**: configure preference to cipher suites defined in the wireless controller
  - **BLE scan state**: enable the BLE scan state
  - **Persistent SSID Broadcast Enable**: enable persistent SSID broadcast
  - **Adr Individual Aggr Enable**: enable the anomaly detection individual report aggregation

- In the **Adr Individual Pc Throttle** field, enter the number of events per client per 5 minutes for anomaly detection individual reports.

  The valid range is from 0 to 50. The default value is 5.

- In the **Adr Individual Pt Throttle** field, enter the number of events per type per 5 minutes for anomaly detection individual reports.

  The valid range is from 0 to 100. The default value is 5.

- (Optional) Under **BLE Beacons**, view the BLE becaon configurations.

  You can manage the BLE beacon configurations through spatial mapping in Cisco Connected Mobile Experiences (CMX) and Cisco Spaces. These attributes are read-only for visibility and alignment with location-based services.

Step 26 Click **Review and Provision**.

Step 27 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 28 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 29 On the **Tasks** window, monitor the task deployment.

Configure global mesh parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global mesh parameters for a wireless controller and provision them.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Mesh**.

Step 4 Click the **Global** tab.

Step 5 (Optional) Under **General**, use the check boxes to enable or disable the corresponding configurations.

- **Ethernet Bridging Allow BPDU**: allow BPDU packets on the mesh network when Ethernet bridging is enabled
- **Subset Channel Sync**: enable synchronization of mesh root AP (RAP) channels across the mobility group
- **Public Safety Enabled**: enable the public safety band

- **Auto DCA RF ASCI APs**: indicate if RRM DCA should always be enabled on the backhaul radio of an RF ASIC-integrated mesh RAP
- **CAC Enabled**: enable the Call Admission Control (CAC) on the mesh AP (MAP)

Step 6 (Optional) Under **Backhaul**, use the check boxes to enable or disable the corresponding configurations.

- **Extended UNII B Domain Channels**: enable the UNII B domain channels in the backhaul radio of MAPs
- **RRM**: enable RRM on the backhaul radio of a root MAP that doesn't have any child MAPs

Step 7 (Optional) Under **Security**, check the **PSK Provisioning** check box to enable PSK provisioning for the MAP.

- (Optional) Check the **Default PSK** check box to enable the default PSK for MAPs.
- From the **PSK Inuse Index** drop-down list, choose a PSK in-use key index.

  To create a PSK key, see Create a mesh PSK for a Cisco Catalyst 9800 Series Wireless Controller, on page 746.

Step 8 Under **Alarm**, enter data in these fields.

- **Max Hop Count**: enter the threshold value for the number of hops from the MAP node to the RAP node for generating the mesh alarm.

  The valid range is from 1 to 16.
- **Recommended Max Children for MAP**: enter the threshold value for the number of children MAPs on a parent MAP for generating the mesh alarm.

  The valid range is from 1 to 50.
- **Recommended Max Children for RAP**: enter the threshold value for the number of children MAPs on a parent RAP for generating the mesh alarm.

  The valid range is from 1 to 50.
- **Parent Change Count**: enter the threshold value for the number of times a child mesh node changes its parent node for generating the mesh alarm.

  The valid range is from 1 to 30.
- **Low Link SNR (dB)**: enter the threshold value for lower SNR on the backhaul link of a child mesh node for generating the mesh alarm.

  The valid range is from 1 to 30.
- **High Link SNR (dB)**: enter the threshold value for higher SNR on the backhaul link of a child mesh node for generating the mesh alarm.

  The valid range is from 31 to 100.
- **Association Count**: enter the threshold value for cumulative association count at the parent mesh node for generating the alarms.

  The valid range is from 1 to 30.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create a mesh PSK for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a mesh preshared key (PSK) for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Mesh**.

Step 4 Click the **PSK Keys** tab.

Step 5 Click **Add**.

Note This option isn't available if five PSK keys are already created.

Step 6 From the **Index** drop-down list of the **Create Mesh Profile Key** slide-in pane, choose an index for the PSK.

Step 7 In the **Psk Key** field, enter the PSK.

The PSK can contain from 3 to 32 characters.

Step 8 From the **Psk Key Type** drop-down list, choose a PSK type.

Step 9 (Optional) In the **Description** field, enter a description for the PSK.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create a mesh profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a mesh profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Mesh**.

Step 4 Click the **Mesh Profiles** tab.

Step 5 Click **Add**.

Step 6 In the **General** tab of the **Create Mesh Profile** slide-in pane, complete these configurations.

a) In the **Mesh Profile Name** field, enter a name for the mesh profile.
b) (Optional) In the **Description** field, enter a description.
c) In the **Range (Root AP to Mesh AP)** field, enter the maximum range between outdoor RAP and MAP.

The valid range is from 150 to 132000. The default value is 12000.

d) From the **Multicast Mode** drop-down list, choose a multicast mode for the Ethernet bridged multicast traffic over mesh networks.
e) (Optional) Check the required check boxes to enable the corresponding configurations.

- **IDS (Rogue/Signature Detection)**: enable the MAP to send IDS and rogue reports to the wireless controller
- **Backhaul Client Access**: enable client access on the backhaul radio of the MAP
- **Background Scanning**: enable background scanning on the backhaul radio of the MAP
- **Battery State for an AP**: enable the external battery state for the MAP
- **Channel Change Notification**: enable the parent MAP to send channel change notification to child MAPs
- **Full Sector DFS Status**: enable full-sector Dynamic Frequency Selection (DFS) on the mesh network
- **LSC**: enable Locally Significant Certificate (LSC) authentication for the MAP
- **Daisychain STP Redundancy**: enable daisy chain Spanning Tree Protocol (STP) redundancy on the MAP
- **Backhaul amsdu**: enable Aggregated MAC Service Data Unit (A-MSDU) on the backhaul radio of the MAP
- **Map Fast Ancestor Find**: enable the MAP fast ancestor find feature on the backhaul radio of the MAP
- **RAP Ethernet Daisy Chain**: enable the RAP Ethernet daisy chain for RAP

f) From the **Convergence Method** drop-down list, choose a convergence method used in the MAPs.

Step 7 Click **Advanced** and complete these configurations.

a) In the **Channel Width** field, enter the backhaul channel width.
b) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Keep Wireless Connection**: allow an AP to retain its wireless connection with the parent AP without switching to a wired channel
- **Least Congested Channel Scan**: enable the least congested channel scan
- **Unii3 Bias**: add a 20% bias towards UNII-3 channels over the other channels
- **Use Unii2**: consider the channels in the UNII-2 band in the least congested channel scan

c) Under **Security**, choose the required option from the corresponding drop-down lists.

From the drop-down list...	Choose...
Method	the security method that is used for MAPs
(Optional) **Authentication Method**	an AAA authentication method list To create an authentication method list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776.
(Optional) **Authorization Method**	an AAA authorization method list To create an authorization method list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

d) (Optional) Under **Ethernet Bridging**, check the required check box to enable the corresponding configurations.

- **VLAN Transparent**: indicate that the Ethernet bridging on MAPs must use the VLAN configuration
- **Ethernet Bridging**: enable Ethernet bridging for MAPs

e) (Optional) Under **Bridge Group**, complete these configurations.

- In the **Bridge Group Name** field, enter a name for the bridge group.
- Check the **Strict Match** check box to enable strict matching of the bridge group name for MAPs for parent selection.

f) Under **5 GHz Band Backhaul**, complete these configurations.

- From the **5 GHz Band Rate Types** drop-down list, choose a backhaul data rate type.
- If you chose the **dot11abg** backhaul data rate type, from the **Rate (Mbps)** drop-down list, choose an enum value for mesh backhaul 802.11 transmission.
- If you chose the **dot11n** backhaul data rate type, in the **Dot11n MCS index** field, enter the 802.11n MCS index for mesh backhaul transmission.

  The valid range is from 0 to 31. The default value is 0.
- If you chose the **dot11ac** backhaul data rate type, you can also configure these optional settings:
  - In the **Dot11ac MCS index** field, enter the 802.11ac MCS index for mesh backhaul transmission.

    The valid range is from 0 to 9. The default value is 0.
  - In the **AC Spatial Stream** field, enter the 802.11ac spatial stream value for mesh backhaul transmission.

    The valid range is from 1 to 4. The default value is 1.
- If you chose the **dot11ax** backhaul data rate type, you can also configure these optional settings:
  - In the **Dot11ax MCS index** field, enter the 802.11ax MCS index for mesh backhaul transmission.

    The valid range is from 0 to 11. The default value is 0.
  - In the **AX Spatial Stream** field, enter the 802.11ax spatial stream value for mesh backhaul transmission.

    The valid range is from 1 to 8. The default value is 1.

g) Under **2.4 GHz Band Backhaul**, complete these configurations.

- From the **2.4 GHz Band Rate Types** drop-down list, choose a backhaul data rate type.
- If you chose the **dot11abg** backhaul data rate type, from the **Rate (Mbps)** drop-down list, choose an enum value for mesh backhaul 802.11 transmission.
- If you chose the **dot11n** backhaul data rate type, in the **Dot11n MCS index** field, enter the 802.11n MCS index for mesh backhaul transmission.

  The valid range is from 0 to 31. The default value is 0.
- If you chose the **dot11ax** backhaul data rate type, you can also configure these optional settings:
  - In the **Dot11ax MCS index** field, enter the 802.11ax MCS index for mesh backhaul transmission.

    The valid range is from 0 to 11. The default value is 0.
  - In the **AX Spatial Stream** field, enter the 802.11ax spatial stream value for mesh backhaul transmission.

    The valid range is from 1 to 4. The default value is 1.

h) (Optional) Under **Fast Roaming**, check the **Fast Teardown** check box to enable fast teardown, and enter data in these fields.

- **Number of Retries**: enter the number of retries until the gateway is considered unreachable.

  The valid range is from 1 to 10. The default value is 4.
- **Interval (seconds)**: enter the retry interval.

  The valid range is from 1 to 10. The default value is 1.
- **Latency Threshold (milliseconds)**: enter the ping latency threshold in milliseconds.

  The valid range is from 1 to 500. The default value is 10.
- **Latency Exceeded Threshold (seconds)**: enter the interval in seconds in which at least one ping must succeed in less than the threshold time.

  The valid range is from 1 to 30. The default value is 8.
- **Uplink Recovery Interval (seconds)**: enter the time in seconds during which the RAP uplink must be stable to accept child connections.

  The valid range is from 1 to 3600. The default value is 60.

Step 8 Click **Review and Provision**.

Step 9 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Option	Description
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create a power profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a power profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Power Profiles**.

Step 4 Click **Add**.

Step 5 In the **Profile Name** field of the **Create Power Profile** slide-in pane, enter a name for the power profile.

Step 6 (Optional) In the **Description** field, enter a description.

Step 7 (Optional) In the **Power Save Client Threshold** field, enter the threshold up to which the AP can stay on the power save mode.

The valid range is from 1 to 32. The default value is 1.

Step 8 (Optional) Under **Rules**, click **Add** to add a rule.

a) In the **Sequence** field, enter a unique interface sequence number.

The valid range is from 0 to 4294967295.

b) From the **Interface** drop-down list, choose an interface.

If you choose...	Then...
Ethernet	complete these configurations: • From the **Interface ID** drop-down list, choose an interface ID. • From the **Parameter Value** drop-down list, choose a parameter value.
Radio	complete these configurations: • From the **Parameter** drop-down list, choose a parameter. • From the **Interface ID** drop-down list, choose an interface ID. • From the **Parameter Value** drop-down list, choose a parameter value. **Note** If you choose the **State** parameter, this drop-down list is disabled.

c) Click **Save**.

Step 9 (Optional) To delete the rules, complete these steps.

a. Check the check box next to the required rules.

b. Hover your cursor over **Actions** and click **Delete**.

c. In the dialog box, click **Yes**.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create a flex profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a flex profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Flex Profiles**.

Step 4 Click **Add**.

Step 5 In the **General** tab of the **Create Flex Profile** slide-in pane, complete these configurations.

a) In the **Flex Profile Name** field, enter a unique name for the flex profile.

The profile name can contain up to 32 characters.

b) (Optional) In the **Description** field, enter a description.
c) In the **Native VLAN ID** field, enter a VLAN ID for the AP.

The valid range is from 1 to 4094. The default value is 1.

d) (Optional) From the **mDNS Flex Profile** drop-down list, choose an mDNS flex profile name.

To create an mDNS flex profile, refer to Create an mDNS flex profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 893.

e) (Optional) Enter data in these fields.

- **HTTP Proxy Port**: enter the HTTP proxy port.

  The valid range is from 0 to 65535. The default value is 0.

- **HTTP Proxy IP Address**: enter the HTTP proxy IP address.

f) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Fallback Radio Shut**: enable the FlexConnect Ethernet Fallback feature for the APs connected to the wireless controller
- **OfficeExtend AP**: use the APs connected to this profile as home APs
- **Flex Resilient**: enable standalone mode support on a Remote-Edge AP (REAP)
- **Join Minimum Latency**: enable the REAP AP to join the wireless controller with minimum latency
- **ARP Caching**: enable ARP cache for the FlexConnect APs connected to the wireless controller
- **IP Overlap**: enable IP overlap support for the site
- **Efficient Image Upgrade**: enable efficient AP image upgrade support
- **Pmk Dist Method**: enable Pairwise Master Key (PMK) distribution with APs

g) (Optional) In the **Maximum Retry Attempts (Secondary)** field, enter the maximum number of retry attempts for secondary devices when trying to establish or maintain a connection.

Increasing the value can improve reliability in unstable environments, but may delay failure detection.

h) (Optional) Under **CTS Policy**, complete these configurations.

- Check the **Inline Tagging** check box to enable Cisco TrustSec (CTS) inline tagging for the FlexConnect APs connected to the wireless controller.
- Check the **SGACL Enforcement** check box to enable CTS role-based enforcement for FlexConnect APs connected to the wireless controller.
- From the **CTS Profile Name** drop-down list, choose a CTS profile.

  To create a profile, refer to Create an SXP AP profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 818.

Step 6 (Optional) Click **Local Authentication** and complete these configurations.

a) From the **RADIUS Server Group** drop-down list, choose a RADIUS server group.

To create a RADIUS server group, refer to Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 770.

b) From the **Local Accounting RADIUS Server Group** drop-down list, choose a RADIUS server group.

To create a RADIUS server group, refer to Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 770.

c) From the **EAP Fast Profile** drop-down list, choose an EAP Fast profile name.

To create an EAP fast profile, refer to Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 800.

d) Check the required check boxes to enable the corresponding configurations.

- **Local Client Roaming**: enable distributed client data caching on AP for local roaming
- **LEAP**: enable the Lightweight Extensible Authentication Protocol (LEAP)
- **TLS**: enable TLS
- **PEAP**: enable the Protected Extensible Authentication Protocol (PEAP)

- **RADIUS**: enable RADIUS

e) Under **Users**, add, edit, or delete the users.

If you want to...	Then...
add a flex local authentication user	click **Add** and complete these steps. **1.** In the **Username** field, enter a username for authenticating a client associated to an AP within the group. **2.** From the **Password Type** drop-down list, choose a password encryption type for authenticating a client associated to an AP within the group. **3.** In the **Password** field, enter a password for authenticating a client associated to an AP within the group. **4.** Click **Save**.
edit a flex local authentication user	**1.** Check the check box next to the required username **2.** Hover your cursor over **Actions**, and click **Edit**. **3.** Edit the required configurations. **4.** Click **Save**.
delete flex local authentication users	**1.** Check the check box next to the required usernames **2.** Hover your cursor over **Actions**, and click **Delete**. **3.** In the dialog box, click **Yes**.

Step 7 (Optional) Click **Policy ACL** and configure the ACLs.

If you want to...	Then...
add a policy ACL	Click **Add** and complete these steps. **a.** From the **ACL Name** drop-down list, choose an ACL. To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785. **b.** To enable central web authentication for the ACL, check the **Central Web Authentication** check box. **c.** In the **URL Filter** field, enter the URL filter list for the ACL. To create URL filters, refer to Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 803 and Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 804. **d.** Click **Save**.

If you want to...	Then...
edit a policy ACL	**a.** Check the check box next to the required policy ACL **b.** Hover your cursor over **Actions**, and click **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete policy ACLs	**a.** Check the check box next to the required policy ACLs **b.** Hover your cursor over **Actions**, and click **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 (Optional) Click **VLAN** and configure VLANs.

If you want to...	Then...
add a VLAN	Click **Add** and complete these steps. **a.** From the **VLAN Name** drop-down list, choose a VLAN name. To create a VLAN, refer to Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 934. **b.** In the **ID** field, enter the VLAN ID to map to the ACL for the AP identified by the VLAN name. The valid range is from 1 to 4096. The default value is 1. **c.** Under **Direction**, click the **Unidirectional** or **Bidirectional** radio button. **d.** If you chose **Unidirectional**, choose an ingress and egress ACL from the corresponding drop-down lists. • **Ingress ACL** (to create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785) • **Egress ACL** (to create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785) **e.** If you chose **Bidirectional**, from the **Acl Name** drop-down list, choose an ACL. To create an ACL, refer to Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785. **f.** Click **Save**.

If you want to...	Then...
edit a VLAN	**a.** Check the check box next to the required VLAN. **b.** Hover your cursor over **Actions**, and click **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete VLANs	**a.** Check the check box next to the required VLANs. **b.** Hover your cursor over **Actions**, and click **Delete**. **c.** In the dialog box, click **Yes**.

Step 9 (Optional) Click **DNS Layer Security** and configure parameter maps.

If you want to...	Then...
add a parameter map	Click **Add** and complete these steps. **a.** In the **Parameter Map Name** field, enter the umbrella profile name. **b.** Click **Save**.
edit a parameter map	**a.** Check the check box next to the required parameter map. **b.** Hover your cursor over **Actions**, and click **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete parameter maps	**a.** Check the check box next to the required parameter maps. **b.** Hover your cursor over **Actions**, and click **Delete**. **c.** In the dialog box, click **Yes**.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Option	Description
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create a site tag for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a site tag for the APs associated with a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Site Tags**.

Step 4 Click **Add**.

Step 5 In the **Site Tag Name** field of the **Create Site Tag** slide-in pane, enter a unique name for the site tag.

The site tag name can contain up to 32 alphanumeric characters and special characters. Catalyst Center does not support leading and trailing spaces in the site tag name.

Step 6 (Optional) In the **Description** field, enter a description.

The description can contain up to 64 alphanumeric characters and special characters.

Step 7 From the **AP Join Profile** drop-down list, choose an AP join profile.

To create an AP join profile, see Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 728.

Step 8 Use the **Local Site** check box to enable or disable the local site.

If this check box is unchecked, from the **Flex Profile** drop-down list, choose a flex profile.

To create a flex profile, see Create a flex profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 753.

Step 9 In the **Load** field, enter an estimate of the relative load contributed by the site.

The valid range is 0 to 1000. The default value is 0.

You can use the AP count for an approximate value.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller

You can set up daily, weekly, or monthly recurrence schedules for calendar profiles. When associated with a power policy, this configuration automates the powering down of interfaces connected to APs. Use this procedure to create a calendar profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **AP** and click **Calendar Profiles**.

Step 4 Click **Add**.

Step 5 In the **Profile Name** field of the **Create Calendar Profile** slide-in pane, enter a name for the calendar profile.

Step 6 Under **Recurrence**, choose the recurrence frequency for the calendar profile.

- **Daily**: applies the calendar profile rules daily.
- **Weekly**: applies the calendar profile rules every week on the selected days. Click the required days to choose them.
- **Monthly**: applies the calendar profile rules every month on the selected dates. Click the required dates to choose them.

Step 7 Under **Start Time** and **End Time**, enter the start time and end time for the recurrence schedule.

Step 8 Click **Review and Provision**.

Step 9 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP priming profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Tag Mapping** and click **AP Priming**.

Step 4 Click **Add**.

Step 5 In the **Profile Name** field of the **Create AP Priming** slide-in pane, enter a name for the priming profile.

Step 6 (Optional) Enter the wireless controller configuration name and the corresponding wireless controller IP address of the AP for these controllers, as required:

- Primary controller
- Secondary controller
- Tertiary controller

Step 7 (Optional) Check the **Geolocation** check box to enable the geographical location for the AP priming profile.

If you enable geographic location for the profile, you can optionally enter data in both these fields:

- **Height (meters)**: enter the height from the ground in meters (rounded to the nearest whole number).

  The valid range is from -100 to 1000.

- **Height Uncertainty (meters)**: enter the height uncertainty in meters.

  The valid range is from 1 to 100.

Step 8 (Optional) Use the **Priming Override** slider to push all the configured priming profile attributes to the AP.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Configure tag priority for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the tag priority for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

Step 4 (Optional) In the **Tag Priority** tab, use the toggle buttons to enable or disable the required configurations.

- **Rule-Based**: enable or disable rule-based tag priority configuration

- **AP**: enable or disable AP-based tag priority configuration

Step 5 (Optional) Check the **AP Tag Persistency** check box to enable persistent AP tags.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create static tag mapping for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create static tag mapping for APs associated with a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

Step 4 Click the **Static** tab.

Step 5 Click **Add**.

Step 6 In the **AP Ethernet MAC Address** field of the **Add Access Point** slide-in pane, enter the Ethernet MAC address of the AP.

Step 7 From these drop-down lists, choose the required tags.

- **Policy Tag**: choose a policy tag for the AP.
- **Site Tag**: choose a site tag for the AP.
- **RF Tag**: choose an RF tag for the AP.

Step 8 From the **Priming Profile** drop-down list, choose an AP priming profile.

To create an AP priming profile, see Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 761.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create a location-based tag-mapping rule for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a location-based tag-mapping rule for APs associated with a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

Step 4 Click the **Location** tab.

Step 5 Click **Add**.

Step 6 In the **General** tab of the **Create Location Rule** slide-in pane, complete these configurations.

a) In the **Location Name** field, enter the name of the AP location.
b) (Optional) In the **Description** field, enter a description.
c) From these drop-down lists, choose the required tags.

- **Site Tag**: choose a site tag for the AP location.
- **Policy Tag**: choose a policy tag for the AP location.
- **RF Tag**: choose an RF tag for the AP location.

Step 7 (Optional) Click **AP Provisioning** and complete these configurations.

If you want to...	Then...
add a nonoperational AP to the rule	**a.** Hover your cursor over **Add** and click **Non-Operational APs**. **b.** In the **AP MAC field** of the **Add AP** dialog box, enter the MAC address of the APs. **c.** Click **Save**.
add an operational AP to the rule	**a.** Hover your cursor over **Add** and click **Operational APs**. **b.** In the **Add AP** dialog box, check the check box next to the APs that you want to add. To search for specific APs, click the Search field and choose the required filter option. Then click **Apply**. **c.** Click **Save**.
delete APs from the rule	**a.** Check the check box next to the APs that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create a rule-based tag-mapping profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a rule-based tag-mapping profile for APs associated with a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Tag Mapping** and click **Tag Mapping**.

Step 4 Click the **Rule-Based** tab.

Step 5 Click **Add**.

Step 6 In the **Rule Name** field of the **Add Regex Rule Profile** slide-in pane, enter a name for the rule.

Step 7 In the **AP Name Regex** field, enter a regular expression for filtering the AP name.

For example, if you have an AP *ap-lab-12*, you can configure the filter with a regular expression, such as **ap-lab**, to match the AP name.

Step 8 (Optional) Use the **Active** toggle button to enable or disable the rule.

If you enable the rule, in the **Priority** field, enter a priority for the rule.

If you enter 0, the rule becomes inactive. You must enter a valid priority value for an active rule.

Step 9 From the **Type** drop-down list, choose either the priming or the tag type.

a) For the **priming** type, choose the priming profile for the AP from the **Priming Profile** drop-down list.

Note To create AP priming profiles, see Create an AP priming profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 761.

b) For the **tag** type, choose the required tags from the following drop-down lists:

- **Policy Tag**: choose a policy tag for the AP.
- **Site Tag**: choose a site tag for the AP.
- **RF Tag**: choose an RF tag for the AP.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Security configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device security configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create a RADIUS server for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a RADIUS server for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **Servers/Groups**, under **RADIUS**, click **Servers**.

Step 5 Click **Add**.

Step 6 In the **Server Name** field of the **Create RADIUS Server** slide-in pane, enter a unique name for the RADIUS server.

Step 7 From the **Type** drop-down list, choose the required type.

Step 8 Based on the type of the RADIUS server, enter data in the corresponding field.

- If the **Server IP Address** field is displayed, enter the IPv4 address for the RADIUS server.
- If the **Server IPv6 Address** field is displayed, enter the IPv6 address for the RADIUS server.
- If the **Server FQDN** field is displayed, enter the FQDN for the RADIUS server.

Step 9 (Optional) Check the **PAC Key** check box to transition from key to Proxy Auto Configuration (PAC) key.

Step 10 Complete these configurations.

If you...	Then...
enabled the PAC key	• From the **PAC Key Type** drop-down list, choose a key type. • In the **PAC Key** field, enter the PAC key for a secure RADIUS server authentication. • In the **Confirm PAC Key** field, confirm the PAC key.
didn't enable the PAC key	• From the **Key Type** drop-down list, choose a key type. • In the **Key** field, enter the key for a secure RADIUS server authentication. • In the **Confirm Key** field, confirm the key.

Step 11 (Optional) Enter data in these fields.

- **Authentication Port**: enter the UDP port number for authentication requests and responses.

  The valid range is from 0 to 65534. The default value is 1812.
- **Accounting Port**: enter the UDP port number for accounting requests and responses.

  The valid range is from 0 to 65534. The default value is 1813.
- **Server Timeout (sec)**: enter the time in seconds to wait for a response from the RADIUS server.

  The valid range is from 1 to 1000.
- **Retry Count**: enter the number of times a client can attempt to retransmit a request to the RADIUS server.

  The valid range is from 0 to 100.

Step 12 (Optional) To enable a change of authorization (CoA) key for dynamic updates to user sessions, check the **Support for CoA** check box.



Note If you chose the type **Hostname**, this check box isn't available.

(Optional) If you check this check box, from the **CoA Server Key Type** drop-down list, choose a key type.

If you chose a CoA server key type, enter data in these fields.

- **CoA Server Key**: enter the CoA server key.
- **Confirm CoA Server Key**: confirm the key.

Step 13 (Optional) Check the **Automate Tester** check box to set up automated network testing.

If you check this check box, complete these configurations.

- In the **Username** field, enter the test user name to include in the RADIUS request.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Ignore Auth Port**: ignore the testing of authentication ports of servers
  - **Ignore Acct Port**: ignore the testing of accounting ports of servers
  - **Enable Probe**: enable probing and send a packet to verify the server status

    If you didn't enable probing, in the **Idle Time (minutes)** field, enter the time, in minutes, after which the server state must be verified.

    The valid range is from 1 to 35791.

Step 14 Click **Review and Provision**.

Step 15 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 16 On the **Tasks** window, monitor the task deployment.

Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a RADIUS server group for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **Servers/Groups**, under **RADIUS**, click **Server Groups**.

Step 5 Click **Add**.

Step 6 In the **Server Group Name** field of the **Create RADIUS Server Group** slide-in pane, enter a name for the RADIUS server group.

Step 7 From the **MAC Delimiter** drop-down list, choose the character for RADIUS compatibility mode.

Step 8 From the **MAC Filtering** drop-down list, choose a MAC filtering option.

Step 9 (Optional) In the **Dead Time (min)** field, enter the time, in minutes, to stop using an unresponsive server.

The valid range is from 0 to 1440.

Step 10 (Optional) Check the **Load Balance** check box to enable load balancing in the RADIUS server group.

Step 11 Choose the IPv4 and IPv6 source interface from the corresponding drop-down lists.

You can choose a physical, logical, or SVI interface for RADIUS traffic.

Step 12 Choose the IPv4 and IPv6 VRF from the corresponding drop-down lists.

Step 13 Under **Servers**, add servers using one of these options.

- Click the plus icon next to the required server.
- Click the required server and click **Add Selected**.

  To choose multiple servers, press **Shift**, click the server, and click **Add Selected**.
- To add all the servers, click **Add All**.

  You can use the **Search** field to filter the servers.

Step 14 Click **Review and Provision**.

Step 15 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 16 On the **Tasks** window, monitor the task deployment.

Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a TACACS+ server for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **Servers/Groups**, under **TACACS+**, click **Servers**.

Step 5 Click **Add**.

Step 6 In the **Server Name** field of the **Create TACACS+ Server** slide-in pane, enter a name for the TACACS+ server.

Step 7 From the **Type** drop-down list, choose the required type.

Step 8 Based on the type of the TACACS+ server, enter data in the corresponding field.

- If the **Server IP Address** field is displayed, enter the IPv4 address for the TACACS+ server.
- If the **Server IPv6 Address** field is displayed, enter the IPv6 address for the TACACS+ server.
- If the **Server FQDN** field is displayed, enter the FQDN for the TACACS+ server.

Step 9 From the **Key Type** drop-down list, choose a key type.

Step 10 In the **Key** field, enter the key for the TACACS+ server for secure authentication.

Step 11 In the **Confirm Key** field, confirm the key for the TACACS+ server.

Step 12 (Optional) In the **Port** field, enter the port number to listen for the incoming requests.

The valid range is from 0 to 65535. The default value is 49.

Step 13 (Optional) In the **Server Timeout (sec)** field, enter the time in seconds to wait for a response from the TACACS+ server.

The valid range is from 1 to 1000.

Step 14 Click **Review and Provision**.

Step 15 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 16 On the **Tasks** window, monitor the task deployment.

Create a TACACS+ server group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a TACACS+ server group for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **Servers/Groups**, under **TACACS+**, click **Server Groups**.

Step 5 Click **Add**.

Step 6 In the **Server Group Name** field of the **Create TACACS+ Server Group** slide-in pane, enter a name for the server group.

Step 7 Choose the IPv4 and IPv6 source interface from the corresponding drop-down lists.

You can choose a physical, logical, or SVI interface for TACACS+ traffic.

Step 8 Choose the IPv4 and IPv6 VRF from the corresponding drop-down lists.

Step 9 Under **Servers**, add servers using one of these options.

- Click the plus icon next to the required server.
- Click the required server and click **Add Selected**.

  To choose multiple servers, press **Shift**, click the server, and click **Add Selected**.
- To add all the servers, click **Add All**.

  You can use the **Search** field to filter the servers.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create an LDAP server for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an LDAP server for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **Servers/Groups**, under **LDAP**, click **Servers**.

Step 5 Click **Add**.

Step 6 In the **Server Name** field of the **Create LDAP Server** slide-in pane, enter a name for the LDAP server.

Step 7 From the **Type** drop-down list, choose the required type.

Step 8 Based on the type of the LDAP server, enter data in the corresponding field.

- If the **Server IP Address** field displays, enter the IPv4 address for the LDAP server.
- If the **Server IPv6 Address** field displays, enter the IPv6 address for the LDAP server.
- If the **Server FQDN** field displays, enter the FQDN for the LDAP server.

Step 9 (Optional) Check the **Authenticate** check box to enable a secure and compliant connection between the wireless controller and the LDAP server.

If you check this check box, enter data in these fields.

- **Bind Username**: enter the user name for the LDAP bind operation.
- **Bind Password**: enter the password for the LDAP bind operation.
- **Confirm Bind Password**: confirm the password for the LDAP bind operation.

Step 10 In the **Port** field, enter the server listening port number.

The valid range is from 1 to 65535. The default value is 389.

Step 11 In the **User Based DN** field, enter the base Distinguished Name (DN).

Step 12 (Optional) In the **Server Timeout (sec)** field, enter the time, in seconds, to wait for a response from the LDAP server before retransmission.

The valid range is from 1 to 65535. The default value is 30.

Step 13 (Optional) Check the **Secure Mode** check box to ensure that the communication between the wireless controller and LDAP server is encrypted.

(Optional) If you check this check box, from the **Trustpoint Name** drop-down list, choose a trustpoint.

Step 14 (Optional) Under **User Object Types**, configure user object types.

If you want to...	Then...
add a user object type	**a.** Click **Add**. **b.** In the **User Object Type** field, enter the object type attribute name. **c.** Click **Save**.
delete user object types	**a.** Check the check box next to the user object types that you want to delete. **b.** Hover your cursor over **Actions** and click **Delete**. **c.** In the dialog box, click **Yes**.

Step 15 Click **Review and Provision**.

Step 16 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 17 On the **Tasks** window, monitor the task deployment.

Create an LDAP server group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an LDAP server group for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **Servers/Groups**, under **LDAP**, click **Server Groups**.

Step 5 Click **Add**.

Step 6 In the **Server Group Name** field of the **Create LDAP Server Group** slide-in pane, enter a name for the server group.

Step 7 Under **Servers**, add servers using one of these options.

- Click the plus icon next to the required server.
- Click the required server and click **Add Selected**.

  To choose multiple servers, press **Shift**, click the server, and click **Add Selected**.
- To add all the servers, click **Add All**.

  You can use the **Search** field to filter the servers.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an authentication method list for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Method List** and click **Authentication**.

Step 5 Hover your cursor over **Add** and choose an authentication type.

- **Type - Login**: for AAA authentication
- **Type - Dot1x**: for web authentication or TACACS

Step 6 In the **Method List Name** field of the **Create Authentication Method List Profile** slide-in pane, enter a name for the authentication method list profile.

Step 7 From the **Group Type** drop-down list, choose an option.

- **Group**: for AAA authentication
- **Local**: for authentication on a local device

Step 8 (Optional) If you chose **Group**, check the **Fallback to Local** check box to use the fallback to the local username authentication.

Step 9 (Optional) From the **Server Groups** drop-down list, choose a server group.

To create a server group, see Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 770 and Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller, on page 771.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an authorization method list for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Method List** and click **Authorization**.

Step 5 Hover your cursor over **Add** and choose an authorization type.

- **Type - Network**
- **Type - Exec**
- **Type - Credential-download**

For MAC filter authorization, choose **Type - Network**.

Step 6 In the **Method List Name** field of the **Create Authorization Method List Profile** slide-in pane, enter a name for the authorization method list profile.

Catalyst Center does not allow spaces or ? in the method list name.

Step 7 Use the **AAA New Model** toggle button to enable or disable the modular approach to AAA.

This setting determines whether the wireless controller applies the new model method for AAA configuration. Advanced security features and integration with external authentication servers require this method.

Step 8 From the **Group Type** drop-down list, choose an option.

- **Group**: for AAA authorization
- **Local**: for authorization on a local device

Step 9 (Optional) If you chose **Group**, check the **Fallback to Local** check box to use the fallback to the local username authentication.

Step 10 (Optional) Check the **Authenticated** check box to indicate success when the authentication is completed.

Step 11 (Optional) From the **Server Groups** drop-down list, choose a server group.

For information about how to create a server group, see Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 770 and Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller, on page 771.

Step 12 Click **Review and Provision**.

Step 13 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 14 On the **Tasks** window, monitor the task deployment.

Create an accounting method list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an accounting method list for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Method List** and choose **Accounting**.

Step 5 Hover your cursor over **Add** and choose an AAA accounting type.

- **Type - Exec**
- **Type - Network**
- **Type - Identity**
- **Type - Command**

For AAA-based accounting, choose **Type - Identity**.

Step 6 In the **Method List Name** field of the **Create Accounting Method List Profile** slide-in pane, enter a name for the accounting method list profile.

Step 7 From the **Server Groups** drop-down list, choose a server group for accounting.

To create a server group, see Create a RADIUS server group for a Cisco Catalyst 9800 Series Wireless Controller, on page 770 and Create a TACACS+ server for a Cisco Catalyst 9800 Series Wireless Controller, on page 771.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure global AAA parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global AAA parameters for a wireless controller and provision them.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Advanced** and choose **Global Configuration**.

Step 5 Under **Global Configurations**, complete these configurations.

- Use the **System Auth Control** check box to enable or disable system authorization control.
- From the **Local Authentication** drop-down list, choose an authentication.

If you chose...	Then...
None	ensure that you choose **None** for local authorization.
Method List	from the **Authentication Method List** drop-down list, choose an authentication method list. To create an authentication method list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776.

- From the **Local Authorization** drop-down list, choose an authorization.

If you chose...	Then...
None	ensure that you choose **None** for local authentication.
Method List	from the **Authorization Method List** drop-down list, choose an authorization method list. To create an authorization method list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

- Use the **RADIUS Server Load Balance** check box to enable or disable load balancing for a RADIUS server.
- Use the **Interim Update** check box to enable or disable interim accounting updates.

Step 6 Under **RADIUS Attributes - Accounting**, complete these configurations.

- From the **Called-station-id** drop-down list, choose the attribute that is appended as the Called-Station-ID.
- From the **Called-station-id Case** drop-down list, choose the capitalization option for the values that are sent on the Called-Station-ID.
- (Optional) From the **MAC Delimiter** drop-down list, choose the character that is used to separate the octets in MAC addresses within accounting records.
- From the **Username Case** drop-down list, choose the capitalization option for the user names.
- From the **Username Delimiter** drop-down list, choose the delimiters for user names.

Step 7 Under **RADIUS Attributes - Authentication**, complete these configurations.

- From the **Called-station-id** drop-down list, choose the attribute that is appended as the Called-Station-ID.
- From the **Called-station-id Case** drop-down list, choose the capitalization option for the values that are sent on the Called-Station-ID.
- From the **MAC Delimiter** drop-down list, choose the character that is used to separate the octets in MAC addresses within accounting records.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a password policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a password policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Advanced** and choose **Password Policy**.

Step 5 Click **Add**.

Step 6 Enter data in these fields of the **Create Password Policy** slide-in pane.

- **Password Policy Name**: enter a name for the password policy.
- **Minimum Length**: enter the minimum length of the password.

  The valid range is from 1 to 127. The default value is 1.
- **Maximum Length**: enter the maximum length of the password.

  The valid range is from 1 to 127. The default value is 127.
- **Upper Count**: enter the number of allowed uppercase letters in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Lower Count**: enter the number of allowed lowercase letters in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Numeric Count**: enter the number of allowed numbers in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Special Count**: enter the number of allowed special characters in the password.

  The valid range is from 0 to 127. The default value is 0.
- **Character Changes**: enter the number of characters that must be changed between the old and new passwords.

  The valid range is from 1 to 127. The default value is 4.
- (Optional) **Max Number of Character Repetition**: enter the maximum number of times for repeating a character consecutively in the password.

  The valid values are 0 and 2–5. The default value is 0. To disable this rule, enter 0.

Step 7 (Optional) Check the **Prohibit Consecutive Four Keyboard Letters** check box to prohibit the use of consecutive characters or numbers on the keyboard in the password.

If you check this check box, the password can't contain four consecutive letters or numbers on the keyboard in both directions.

Step 8 From the **Validity** drop-list, choose a validity for the password.

For the user-defined validity, enter data in these fields:

- **Years**: enter the number of years for password expiration.

  The valid range is from 0 to 99.

- **Months**: enter the number of months for password expiration.

  The valid range is from 0 to 11.

- **Days**: enter the number of days for password expiration.

  The valid range is from 0 to 30.

- **Hours**: enter the number of hours for password expiration.

  The valid range is from 0 to 23.

- **Minutes**: enter the number of minutes for password expiration.

  The valid range is from 0 to 59.

- **Seconds**: enter the number of seconds for password expiration.

  The valid range is from 0 to 59.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Configure RADIUS fallback for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure RADIUS fallback for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Advanced** and choose **RADIUS Fallback**.

Step 5 (Optional) Enter data in these fields.

- **Retransmit Count**: enter the number of retries to the active server.

  The valid range is from 0 to 100.

- **Timeout Interval (sec)**: enter the time, in seconds, to wait for a RADIUS server to reply.

  The valid range is from 1 to 1000.

- **Dead Time (min)**: enter the time, in minutes, to stop using an unresponsive server.

  The valid range is from 1 to 1440.

- **Dead Criteria Time (sec)**: enter the time, in seconds, to determine how quickly the system switches to a backup server to ensure uninterrupted network authentication and access.

  The valid range is from 1 to 120.

- **Dead Criteria Retries**: enter the required number of consecutive response failures from the RADIUS server to the router to mark the RADIUS server as inactive.

  The valid range is from 1 to 100.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an attribute list for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA**.

Step 4 Hover your cursor over **AAA Advanced** and choose **Attribute Lists**.

Step 5 Click **Add**.

Step 6 In the **Attribute List Name** field of the **Create Attribute List** slide-in pane, enter a name for the attribute list.

Step 7 (Optional) Under **Attributes**, configure the required attributes.

If you want to...	Then...
add an attribute	**a.** Click **Add**. **b.** In the **Add Attribute** dialog box, enter data in these fields. • **Attribute Type**: enter the name of the attribute type for streamlined user access control. Alternatively, when you start typing, the list of available attribute types is displayed. You can choose the required attribute type from this list. • **Attribute Value**: enter the value associated with the chosen attribute type. Alternatively, if the **Attribute Value** drop-down list is displayed, choose the required value. **c.** Click **Save**.
delete attributes	**a.** Check the check box next to the required attributes. **b.** Hover your cursor over **Actions**, and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an AAA policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AAA policy profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AAA Policy**.

Step 4 Click **Add**.

Step 5 In the **Policy Name** field of the **Create AAA Policy Profile** slide-in pane, enter a name for the AAA policy.

Step 6 From the NAS ID option drop-down lists, choose the required RADIUS NAS ID options.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 ACL for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **ACL**.

Step 4 Hover your cursor over **IPv4/IPv6**, under **IPv4**, choose **Standard**.

Step 5 Click **Add**.

Step 6 In the **ACL Name** field of the **Create IPv4 Standard ACL** slide-in pane, enter a unique name for the IPv4 ACL.

The ACL name can contain up to 231 alphanumeric characters and special characters. If you're entering only numbers, the valid range is either 1 to 99 and 1300 to 1999. If the ACL name has a special character, it must start with an alphabetic character. Catalyst Center does not support ? and spaces in the ACL name.

Step 7 (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is from 1 to 2147483647.
3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source IPv4 address.
   - **Host**: applies to traffic from a specific IPv4 address.

     If you choose **Host**, in the **Source IP** field, enter the IP address of a source host. Catalyst Center does not support 0.0.0.0 as the IP address of a source host.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Subnet IP**: Enter the subnet IP address. Catalyst Center does not support 0.0.0.0 as the subnet IP address.
     - **Source Wildcard**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0.0.0.0 as the wildcard.
5. (Optional) Check the **Log** check box to create logs for matches against this entry.
6. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.

2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an IPv4 role-based ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 role-based ACL for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **ACL**.

Step 4 Hover your cursor over **IPv4/IPv6**, under **IPv4**, choose **Role-based**.

Step 5 Click **Add**.

Step 6 In the **ACL Name** field of the **Create IPv4 Role-based ACL** slide-in pane, enter a unique name for the IPv4 ACL.

The ACL name can contain up to 229 alphanumeric characters and special characters. If the ACL name has a special character, it must start with an alphabetic character. Catalyst Center does not support ? and spaces in the ACL name.

Step 7 (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 2147483647.
3. From the **Action** drop-down list, choose an action.

- **permit**: allow the traffic
- **deny**: block the traffic

4. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:

   - **Source Port Operator**: choose a source port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

   - **Destination Port Operator**: choose a destination port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

5. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
6. (Optional) Check the **Log** check box to create logs for matches against this entry.
7. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an IPv4 extended ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 extended ACL for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **ACL**.

Step 4 Hover your cursor over **IPv4/IPv6**, under **IPv4**, choose **Extended**.

Step 5 Click **Add**.

Step 6 In the **ACL Name** field of the **Create IPv4 Extended ACL** slide-in pane, enter a unique name for the IPv4 extended ACL.

The ACL name can contain up to 231 alphanumeric characters and special characters. If you're entering only numbers, the valid range is either 1 to 99 or 1300 to 1999. If the ACL name has a special character, it must start with an alphabetic character. Catalyst Center doesn't support ? and spaces in the ACL name.

Step 7 (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 2147483647.
3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source IPv4 address.
   - **Host**: applies to traffic from a specific IPv4 address.

     If you choose **Host**, in the **Source IP** field, enter the IP address of a source host. Catalyst Center does not support 0.0.0.0 as the IP address of a source host.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Subnet IP**: Enter the subnet IP address. Catalyst Center does not support 0.0.0.0 as the subnet IP address.
     - **Source Wildcard**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0.0.0.0 as the wildcard.
5. From the **Destination Type** drop-down list, choose a traffic destination to apply for the rule.
   - **Any**: applies to traffic to any destination IPv4 address.
   - **Host**: applies to traffic to a specific IPv4 address.

     If you choose **Host**, in the **Destination IP** field, enter the IP address of a destination host. Catalyst Center does not support 0.0.0.0 as the IP address of a destination host.
   - **Network**: applies to traffic to a network.

     If you choose **Network**, enter data in these fields:
     - **Subnet IP**: Enter the subnet IP address. Catalyst Center does not support 0.0.0.0 as the subnet IP address.

- **Destination Wildcard**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0.0.0.0 as the wildcard.

6. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:

   - **Source Port Operator**: choose a source port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

   - **Destination Port Operator**: choose a destination port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

7. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
8. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv6 ACL for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **ACL**.

Step 4 Hover your cursor over **IPv4/IPv6**, under **IPv6**, choose **IPv6**.

Step 5 Click **Add**.

Step 6 In the **ACL Name** field of the **Create IPv6 ACL** slide-in pane, enter a unique name for the IPv6 ACL.

The ACL name can contain up to 233 alphanumeric characters and special characters. It must not start with a number. Catalyst Center doesn't support ? and spaces in the ACL name.

Step 7 (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 4294967294.
3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source IPv6 address.
   - **Host**: applies to traffic from a specific IPv6 address.

     If you choose **Host**, in the **Source IP** field, enter the valid IPv6 address of a source host. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as the IPv6 address.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Source IP**: Enter the source subnet IP address. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: for the IPv6 address.
     - **Source Wildcard Bits**: enter the wildcard bits to apply to the source. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as a value in this field.
5. From the **Destination Type** drop-down list, choose a traffic destination to apply for the rule.
   - **Any**: applies to traffic to any destination IPv6 address.
   - **Host**: applies to traffic to a specific IPv6 address.

     If you choose **Host**, in the **Destination IP** field, enter the IP address of a destination host. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as the IPv6 address.
   - **Network**: applies to traffic to a network.

     If you choose **Network**, enter data in these fields:
     - **Destination IP**: Enter the destination subnet IP address. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as the IPv6 address.
     - **Destination Wildcard Bits**: enter the wildcard bits to apply to the destination. Catalyst Center does not support 0000:0000:0000:0000:0000:0000:0000:0000 or :: as a value in this field.

6. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:

   - **Source Port Operator**: choose a source port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

   - **Destination Port Operator**: choose a destination port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

7. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
8. (Optional) Check the **Log** check box to create logs for matches against this entry.

9. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an IPv6 role-based ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv6 role-based ACL for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **ACL**.

Step 4 Hover your cursor over **IPv4/IPv6**, under **IPv6**, choose **Role-based**.

Step 5 Click **Add**.

Step 6 In the **ACL Name** field of the **Create IPv6 Role-based ACL** slide-in pane, enter a unique name for the IPv6 ACL.

The ACL name can contain up to 222 alphanumeric characters and special characters. It must not start with a number. Catalyst Center doesn't support ? and spaces in the ACL name.

Step 7 (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. In the **Sequence** field of the **Add Rule** dialog box, enter a unique integer for the rule index.

   The valid range is 1 to 4294967294.
3. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
4. In the **Protocol** field, specify a protocol to apply for the rule. You can enter a number in the range 0 to 255 or an IOS keyword such as bgp, tcp, udp, and so on.

   If you use TCP or UDP, choose a port operator to specify how the port numbers are evaluated from these drop-down lists:

   - **Source Port Operator**: choose a source port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Source Port** field, enter the source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.
range	Enter the range of port numbers in these fields: • **Start Source Port**: enter the starting source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Source Port**: enter the ending source port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

   - **Destination Port Operator**: choose a destination port operator.

If you choose...	Then...
eq, **gt**, **lt**, or **neq**	In the **Destination Port** field, enter the destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

If you choose...	Then...
range	Enter the range of port numbers in these fields: • **Start Destination Port**: enter the starting destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535. • **End Destination Port**: enter the ending destination port number or an IOS service keyword such as bgp, bootpc, tacacs, and so on. Both port number and IOS service keyword are validated against the same numeric range. The valid range is 0 to 65535.

5. (Optional) From the **Dscp** drop-down list, choose a DSCP value for the rule.
6. (Optional) Check the **Log** check box to create logs for matches against this entry.
7. Click **Save**.

b) To edit a rule, complete these steps:

1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:

1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a MAC-based ACL for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a MAC-based ACL for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **ACL**.

Step 4 Click the **MAC-Based** tab.

Step 5 Click **Add**.

Step 6 In the **ACL Name** field of the **Create MAC-Based ACL** slide-in pane, enter a unique name for the MAC-based ACL.

The ACL name can contain up to 230 alphanumeric characters and special characters. Catalyst Center doesn't support ? and spaces in the ACL name. If the ACL name has an alphanumeric or special character, it must start with an alphabetic character.

Step 7 (Optional) Under **Rules**, configure the required rules.

a) To create a rule, complete these steps:

1. Click **Add**.
2. From the **Action** drop-down list, choose an action.
   - **permit**: allow the traffic
   - **deny**: block the traffic
3. From the **Source Type** drop-down list, choose a traffic source to apply for the rule.
   - **Any**: applies to traffic from any source MAC address.
   - **Host**: applies to traffic from a specific MAC address.

     If you choose **Host**, in the **Source MAC** field, enter the source MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
   - **Network**: applies to traffic from a network.

     If you choose **Network**, enter data in these fields:
     - **Source MAC**: Enter the source MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
     - **Source MAC Wildcard**: enter the wildcard bits to apply to the source. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.

4. From the **Destination Type** drop-down list, choose a traffic destination to apply for the rule.
   - **Any**: applies to traffic to any destination MAC address.
   - **Host**: applies to traffic to a specific MAC address.

     If you choose **Host**, in the **Destination MAC** field, enter the destination MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
   - **Network**: applies to traffic to a network.

     If you choose **Network**, enter data in these fields:
     - **Destination MAC**: Enter the destination MAC address. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
     - **Destination MAC Wildcard**: enter the wildcard bits to apply to the destination. Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xx:xx:xx:xx:xx:xx* format.
5. Click **Save**.

b) To edit a rule, complete these steps:
1. Check the check box next to the required rule.
2. Hover your cursor over **Actions**, and choose **Edit**.
3. Edit the required configurations.
4. Click **Save**.

c) To delete rules, complete these steps:
1. Check the check box next to the required rules.
2. Hover your cursor over **Actions**, and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:
- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a local EAP profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a local EAP profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **EAP**.

Step 4 In the **Local EAP Profiles** tab, click **Add**.

Step 5 In the **Local EAP Profile Name** field of the **Create Local EAP Profiles** slide-in pane, enter a unique name for the local EAP profile.

The profile name can contain up to 63 alphanumeric and special characters.

Step 6 (Optional) Check the required check boxes to allow the corresponding EAP methods.

Step 7 (Optional) Based on the EAP method that you chose, complete these configurations.

If you chose...	Then...
EAP-TLS, **EAP-FAST**, or **PEAP**	from the **Trustpoint Name** drop-down list, choose a default PKI trustpoint.
EAP-FAST	from the **EAP-FAST Profile** drop-down list, choose an EAP FAST profile. To create an EAP FAST profile, see Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 800.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an EAP-FAST profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EAP-FAST profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **EAP**.

Step 4 Click the **EAP-FAST Profiles** tab.

Step 5 Click **Add**.

Step 6 In the **Create EAP-FAST Profiles** slide-in pane, enter data in these fields.

- **EAP-FAST Profile Name**: enter a unique name for the EAP-FAST profile.

  The profile name can contain up to 63 alphanumeric and special characters.

- **Server Key**: enter a local key for the profile.
- **Confirm Server Key**: reenter the same local key for the profile.
- **Time to Live (sec)**: enter the Protected Access Credential (PAC) time-to-live in seconds.

  The valid range is 1 to 700000000. The default value is 86400.

- (Optional) **Authority ID**: enter an authority ID for the profile.

  The authority ID can contain up to 231 alphanumeric and special characters.

- (Optional) **Authority ID Information**: enter the authority ID information.

  The authority ID information can contain up to 228 alphanumeric and special characters.

- (Optional) **Description**: enter a description.

  The description can contain up to 241 alphanumeric and special characters.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure advanced EAP for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the advanced EAP profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **EAP**.

Step 4 Click the **Advanced** tab.

Step 5 Enter data in these fields.

- **EAP-Identity-Request Timeout (sec)**: enter an EAP identity request timeout in seconds.

  The valid range is from 1 to 120. The default value is 40.

- **EAP-Identity-Request Max Retries**: enter the maximum number of EAP identity request retransmissions.

  The valid range is from 1 to 20. The default value is 2.

Step 6 (Optional) Check the **EAP Max-Login Ignore Identity Response** check box to limit the number of clients that can be connected to the device with the same username.

Step 7 Enter data in these fields.

- **EAP-Request Timeout (sec)**: enter the EAP request retransmission timeout in seconds.

  The valid range is from 1 to 120. The default value is 30.

- **EAP-Request Max Retries**: enter the maximum number of EAP request retransmissions.

  The valid range is from 0 to 20. The default value is 2.

- **EAPOL-Key Timeout (msec)**: enter the EAP over LAN (EAPOL) key retransmission timeout in milliseconds.

  The valid range is from 200 to 5000. The default value is 1000.

- **EAPOL-Key Max Retries**: enter the maximum number of EAPOL key retries.

  The valid range is from 0 to 4. The default value is 2.

- **EAP-Broadcast Key Interval (sec)**: enter the EAP broadcast key renewal interval in seconds.

  The valid range is from 120 to 86400. The default value is 3600.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a basic URL filter for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a basic URL filter for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **URL Filters**.

Step 4 In the **Basic** tab, click **Add**.

Step 5 In the **Url List Name** field of the **Create Basic URL Filter** slide-in pane, enter a unique name for the URL filter.

The URL filter name can contain up to 32 characters. Catalyst Center does not support ? # % + ' or spaces in the URL filter name.

Step 6 From the **Filter Type** drop-down list, choose the authentication that is used for the URL filter.

If you chose **POST-AUTH**, enter data in these fields.

- **IPv4 Redirect Server**: enter the IPv4 address of the redirect server.
- **IPv6 Redirect Server**: enter the IPv6 address of the redirect server.

Step 7 From the **Action** drop-down list, choose an action to indicate if the URLs in the URL filter are allowed or blocked.

Step 8 (Optional) Under **URLs**, configure URL domain names for the URL filter.

If you want to...	Then...
add a URL domain name to the URL filter	**a.** Click **Add**. **b.** In the **Url Name** field of the **Add URL** dialog box, enter a domain name for the URL filter. The domain name can contain up to 255 characters. Catalyst Center supports the special characters - _ . and * in the domain name. * is used as a wildcard character (for example, *cisco.com). Catalyst Center does not support subdomains using backslash (/). **c.** Click **Save**.
delete domain names from the URL filter	**a.** Check the check box next to the domain names that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create an enhanced URL filter for a Cisco Catalyst 9800 Series Wireless Controller

Enhanced URL filters are the Fully Qualified Domain Name (FQDN) ACLs that are applied to the wireless network.

Use this procedure to create an enhanced URL filter for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **URL Filters**.

Step 4 Click the **Enhanced** tab.

Step 5 Click **Add**.

Step 6 In the **Url List Name** field of the **Create Enhanced URL Filter** slide-in pane, enter a unique name for the enhanced URL filter.

The URL filter name can contain up to 32 characters. Catalyst Center does not support ? # % + ' or spaces in the URL filter name.

Step 7 (Optional) Under **Rules**, configure rules for the URL filter.

If you want to...	Then...
add a rule	**a.** Click **Add**. **b.** In the **URL** field of the **Add URL** dialog box, enter a URL, FQDN, or domain name for the enhanced URL rule. The domain name can contain up to 255 characters. Catalyst Center supports the special characters - _ . and * in the domain name. * is used as a wildcard character (for example, *cisco.com). Catalyst Center does not support subdomains using backslash (/). **c.** In the **Preference** field, enter a priority for the rule. The valid range is from 0 to 65535. **d.** Click **Save**. **e.** From the **Action** drop-down list, choose an action.
edit a rule	**a.** Check the check box next to the required rule. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** From the **Action** drop-down list, update the action for the rule. **d.** Click **Save**.
delete rules	**a.** Check the check box next to the rules that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a guest user for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a guest user for a wireless controller and provision.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Guest User**.

Step 4 Click **Add**.

Step 5 In the **Create Guest User** slide-in pane, under **General**, complete these configurations.

- In the **User Name** field, enter a username for the guest user.
- (Optional) Check the **Generate Password** check box to generate a password for the guest user.
- In the **Password** field, enter a password for the guest user.

  Note If you check the **Generate Password** check box, this field is automatically populated.

- In the **Confirm Password** field, reenter the password.

  Note If you check the **Generate Password** check box, this field is automatically populated.

- In the **Description** field, enter a description.
- In the **No. of Simultaneous User Logins** field, enter the maximum allowed simultaneous login attempts for the guest user.

  The valid range is from 0 to 64.

Step 6 Under **Lifetime**, enter data in these fields.

- **Years**: enter the number of years for which the guest user credentials can be used.

  The valid range is from 0 to 1. The default value is 0.

- **Months**: enter the number of months for which the guest user credentials can be used.

  The valid range is from 0 to 11. The default value is 0.

- **Days**: enter the number of days for which the guest user credentials can be used.

  The valid range is from 0 to 30. The default value is 1.

- **Hours**: enter the number of hours for which the guest user credentials can be used.

  The valid range is from 0 to 23. The default value is 0.

- (Optional) **Minutes**: enter the number of minutes for which the guest user credentials can be used.

  The valid range is from 0 to 59. The default value is 0.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure web authentication parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the web authentication parameters for a wireless controller and provision.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Web Auth**.

Step 4 In the **Global** tab, complete these configurations.

a) Under **General**, complete these configurations.

- (Optional) In the **Maximum HTTP Connections** field, enter the maximum number of allowed HTTP connections per client.

  The valid range is from 1 to 200.

- In the **Init-State Timeout(Secs)** field, enter the timeout in seconds.

  The valid range is from 60 to 3932100.

- From the **Type** drop-down list, choose the authentication type.
- (Optional) If you chose the authentication type **consent**, check the **Turn-On Consent with Email** check box to enable consent with email.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Captive Bypass Portal**: enable captive bypassing for web authentication
  - **Disable Success Window**: disable the default success window for the wireless controller after successful web authentication
  - **Disable Logout Window**: disable the web authentication logout window
  - **Disable Cisco Logo**: disable the Cisco logo on internal HTML windows
- (Optional) Enter data in these fields.
  - **Sleeping Client Timeout (Minutes)**: enter the client sleep timeout in minutes.

    The valid range is from 10 to 43200.
  - **Trustpoint**: enter the trustpoint name.
  - **Virtual IPv4 Address**: enter the virtual IPv4 address.
  - **Virtual IPv6 Address**: enter the virtual IPv6 address.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Web Auth intercept HTTPS**: enable the interception of the HTTPS traffic
  - **Enable HTTP server for Web Auth**: configure an HTTP server for web authentication
  - **Disable HTTP secure server for Web Auth**: disable the HTTPS server for web authentication

b) (Optional) Under **Banner Configuration**, complete these configurations.

- In the **Banner Title** field, enter the text for the banner title.

  You can enter up to 127 characters. For example, *c* **banner-title-text** *c*, where *c* is a delimiter.
- Under **Banner Type**, click the radio button next to the required option.

If you chose...	Then...
Banner Text	in the **Banner Text** field, enter the text to display in the banner. You can enter up to 400 characters. For example, *c* **banner-text** *c*, where *c* is a delimiter.
File Name	in the **Read from File** field, enter the name of the file from which the banner text can be read.

c) (Optional) Under **Redirect to external server**, enter data in these fields for external web authentication.

- **Redirect URL for login**: enter the URL to redirect the user for a login request.

  You can enter up to 230 characters.

- **Redirect On-Success**: enter the URL to redirect the user after a successful login.

  You can enter up to 230 characters.

- **Redirect On-Failure**: enter the URL to redirect the user after a failed login.

  You can enter up to 230 characters.

- **Redirect Append for AP MAC Address**: enter the AP MAC address to be appended to the redirection.
- **Redirect Append for Client MAC Address**: enter the client MAC address to be appended to the redirection.
- **Redirect Append for WLAN SSID**: enter the WLAN SSID to be appended to the redirection.
- **Portal IPV4 Address**: enter the IPv4 address of the portal to send redirects.
- **Portal IPV6 Address**: enter the IPv6 address of the portal to send redirects, if the IPv6 address is used.

d) (Optional) Under **Customized page**, enter data in these fields for customized web authentication.

- **Login Page**: enter the file details for the customized login window for web authentication in the *bootflash:filename* format.
- **Logout Page**: enter file details for the customized logout window for web authentication in the *bootflash:filename* format.
- **Login Successful Page**: enter the file details for the customized window for a successful login in the *bootflash:filename* format.
- **Login Failed Page**: enter the file details for the customized window for a failed login in the *bootflash:filename* format.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a web authentication profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Web Auth**.

Step 4 Click the **Web Auth Profiles** tab.

Step 5 Click **Add**.

Step 6 In the **General** tab of the **Create Web Auth** slide-in pane, complete these configurations.

- In the **Parameter Map Name** field, enter a name for the web authentication profile.
- (Optional) In the **Maximum HTTP connections** field, enter the maximum number of allowed HTTP connections.

  The valid range is from 1 to 200.
- From the **Type** drop-down list, choose an authentication type: **authbypass**, **webauth**, **consent**, or **webconsent**
- (Optional) In the **Init-State Timeout(secs)** field, enter the web authentication timeout in seconds.

  The valid range is from 60 to 3932100.
- (Optional) Check the **Sleeping Client Status** check box to enable authentication of sleeping clients.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

What to do next

To configure additional parameters for the web authentication profile, refer to Configure web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 811.

Configure web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure additional parameters for web authentication profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Web Auth**.

Step 4 Select the web authentication profile for which you want to configure additional parameters:

a) Click the **Web Auth Profiles** tab.
b) Check the check box for the required web authentication profile.
c) Hover your cursor over **Actions** and choose **Edit**.

Step 5 In the **General** tab of the **Edit Web Auth** slide-in pane, complete these configurations.

a) Under **General**, complete these configurations:

- (Optional) In the **Maximum HTTP connections** field, enter the maximum number of allowed HTTP connections.

  The valid range is from 1 to 200.

- From the **Type** drop-down list, choose an authentication type: **authbypass**, **webauth**, **consent**, or **webconsent**
- (Optional) In the **Init-State Timeout(secs)** field, enter the web authentication timeout in seconds.

  The valid range is from 60 to 3932100.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Captive Bypass Portal**: enable captive bypassing for web authentication
  - **Disable Success Window**: disable the default success window for the wireless controller after successful web authentication
  - **Disable Logout Window**: disable the web authentication logout window
  - (Optional) Check the **Sleeping Client Status** check box to enable authentication of sleeping clients.

    If you enable this option, in the **Sleeping Client Timeout (minutes)** field, you can optionally enter the sleep timeout in minutes.

    The valid range is from 10 to 43200 minutes.

b) (Optional) Under **Banner Configuration**, complete these configurations.

- In the **Banner Title** field, enter the text for the banner title.

The title can contain up to 127 characters.

- Under **Banner Type**, select the required option: **None**, **Banner Text**, or **File Name**.

If you chose...	Then...
Banner Text	in the **Banner Text** field, enter the text to display in the banner. For example, *c* **banner-text** *c*, where *c* is a delimiter.
Read From File	in the **File Name** field, enter the name of the file from which the banner text can be read. The file name can contain up to 61 characters.

Step 6 In the **Advanced** tab, complete these configurations:

a) (Optional) Under **Redirect to external server**, enter data in these fields for external web authentication.

- **Redirect URL for login**: enter the URL to redirect the user for a login request.

  You can enter up to 230 characters. Catalyst Center does not allow spaces in the URL.

- **Redirect On-Success**: enter the URL to redirect the user after a successful login.

  You can enter up to 230 characters. Catalyst Center does not allow spaces in the URL.

- **Redirect On-Failure**: enter the URL to redirect the user after a failed login.

  You can enter up to 230 characters. Catalyst Center does not allow spaces in the URL.

- **Redirect Append for AP MAC Address**: enter the redirect append for the AP MAC address to be appended to the redirect ACL.

  You can enter up to 227 characters. Catalyst Center does not allow spaces and ? in the redirect append.

- **Redirect Append for Client MAC Address**: enter the redirect append for the client MAC address to be appended to the redirect ACL.

  You can enter up to 223 characters. Catalyst Center does not allow spaces and ? in the redirect append.

- **Redirect Append for WLAN SSID**: enter the redirect append for the WLAN SSID to be appended to the redirect ACL.

  You can enter up to 224 characters. Catalyst Center does not allow spaces and ? in the redirect append.

- **Portal IPV4 Address**: enter the IPv4 address of the portal to send redirects.

  Enter the IP address in the *xxx.xxx.xxx.xxx* format.

- **Portal IPV6 Address**: enter the IPv6 address of the portal to send redirects, if the IPv6 address is used.

  Enter the IP address in the *X:X:X:X:X:X:X:X* format.

b) (Optional) Under **Customized page**, enter data in these fields for customized web authentication.

- **Login Page**: enter the file details for the customized login window for web authentication in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

- **Logout Page**: enter file details for the customized logout window for web authentication in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

- **Login Successful Page**: enter the file details for the customized window for a successful login in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

- **Login Failed Page**: enter the file details for the customized window for a failed login in the *bootflash:filename* format.

  File details must start with *bootflash:*, *harddisk:*, or *flash:*.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure CTS for a Cisco Catalyst 9800 Series Wireless Controller

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

Use this procedure to configure Cisco TrustSec (CTS) for a Cisco Catalyst 9800 Series Wireless Controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Trustsec**.

Step 4 In the **Global** tab, configure the Cisco TrustSec (CTS) parameters.

Step 5 (Optional) In the **CTS Device ID** field, enter a name for the TrustSec network access device.

The name can contain up to 32 characters. The name must be same as the name configured in Cisco Identity Services Engine.

Step 6 (Optional) In the **CTS Password**, enter a password for the CTS.

The password can contain up to 162 characters. Catalyst Center does not support ? and spaces in the password.

Step 7 (Optional) From the **CTS Authorization List** drop-down list, choose a list of AAA servers for the TrustSec device.

To create an authorization list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

Step 8 (Optional) In the **CTS Device SGT** field, enter a number for the local device security group.

The valid range is from 2 to 65519. For Cisco IOS XE Release 17.17.1 or later, the valid range is from 2 to 65521.

Step 9 (Optional) Under **Policy Server Configuration**, complete these configurations:

- In the **Device Name** field, enter the name of the device used in Cisco ISE.
- In the **Username** field, enter the user name.

  The user name can contain up to 32 characters.
- From the **Encryption** drop-down list, choose the encryption type for the password.
- In the **Password** field, enter the password.

  The password can contain up to 24 characters.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

What to do next

In the **Policy Servers** table, you can optionally add, edit, or delete policy servers. To add a policy server, see Create a policy server for CTS configuration, on page 814.

Create a policy server for CTS configuration

Use this procedure to create a policy server for CTS policy server configuration for a Cisco Catalyst 9800 Series Wireless Controller and provision it.

For information about CTS configuration for a wireless controller, see Configure CTS for a Cisco Catalyst 9800 Series Wireless Controller, on page 813.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Trustsec**.

Step 4 In the **Global** tab, under **Policy Servers** table, click **Add**.

Step 5 In the **Create Policy Server** slide-in pane, under **Policy Server Profile**, complete these configurations:

- In the **Policy Server Profile Name** field, enter a unique name for the policy server profile.

  The profile name can contain up to 255 characters. Catalyst Center does not support question mark (?) and spaces in the profile name. This name identifies the policy server configuration in the wireless controller.

- (Optional) In the **Domain Name** field, enter the Fully Qualified Domain Name (FQDN) of the policy server. To use DNS resolution, use this name instead of an IP address.

  The domain name can contain up to 128 characters.

- (Optional) In the **Server Port** field, enter the port number that is used to connect to the policy server.

  The valid range is from 1025 to 65535. Ensure that this port matches the listening port configured on the policy server.

- (Optional) In the **Retransmit Attempts** field, enter the number of times the wireless controller retries sending a request to the policy server if it does not receive a response.

  The valid range is from 0 to 5. A higher value increases reliability but may delay failure detection.

- (Optional) In the **Timeout (seconds)** field, enter the time, in seconds, that the wireless controller waits before considering this attempt as a failed attempt.

  The valid range is from 1 to 60.

- From the **TLS Server Trustpoint** drop-down list, choose a TLS server trustpoint.

- (Optional) If available, use the **Use JSON Content Type** toggle button to enable or disable the usage of JSON as the content type for communication with the policy server.

Step 6 Under **IP Address**, configure IP address.

If you want to...	Then...
add an IP address	**a.** Click **Add**. **b.** In the **IP Address** field of the **Add IP Address** dialog box, enter a valid IPv4 or IPv6 address.
delete IP addresses	**a.** Check the check box for the IP addresses that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure SXP for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure SGT Exchange Protocol (SXP) for Cisco TrustSec (CTS) for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Trustsec**.

Step 4 (Optional) In the **SXP** tab, complete these configurations.

a) Use the **SXP Status** toggle button to enable or disable the support for CTS SXP.
b) Configure these parameters:

- **Default SXP Source IPv4 Address**: enter a valid default SXP source IPv4 address.

- **Default SXP Password Type**: choose a default SXP password type.
- **Default SXP Password**: enter a default SXP password.

  The password can contain up to 162 characters.
- **Reconciliation Period (sec)**: enter the reconciliation time in seconds.

  The valid range is from 0 to 64000.
- **Retry Period (sec)**: enter the retry period for SXP connection in seconds.

  The valid range is from 0 to 64000.
- **Source Ipv6**: enter a valid source IPv6 address.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

What to do next

If you enable the support for CTS SXP, in the **Peer Connections** table, you can optionally add, edit, or delete the peer connections.

To add a peer connection, click **Add** and complete these configurations.

1. From the **Mode of Local Device** drop-down list, choose a role for the local device.
2. From the **IP Type** drop-down list, choose an IP address type.
3. In the **Peer IP** field, enter an SXP peer IP address based on the selected IP address type.
4. (Optional) In the **Source IP** field, enter an SXP source IP address based on the selected IP address type.
5. From the **Password** drop-down list, choose a type of password.
6. Complete Step 5, on page 817 to Step 7, on page 817.

Create a CTS link configuration for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a CTS link configuration for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Trustsec**.

Step 4 In the **CTS Link Configuration** tab, click **Add**.

Step 5 In the **Create CTS Link Configuration** slide-in pane, complete these configurations:

a) (Optional) From the **Interface Name** drop-down list, choose an interface.
b) Use the **CTS Manual** toggle button to enable or disable the CTS manual mode.

If you enable the CTS manual mod, complete the required configurations.

- In the **Port SGT** field, enter the source Security Group Tag (SGT) number to apply to untagged or nontrusted incoming traffic.

  The valid range is from 2 to 65519.

- (Optional) Check the **Trusted** check box to trust the source SGT that the peer uses for sending.
- Use the **Propagate SGT** toggle button to configure CTS SGT propagation configuration.

Note If you check the **Trusted** check box, this option is dimmed.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an SXP AP profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a CTS SXP AP profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Trustsec**.

Step 4 Click the **AP** tab.

Step 5 Click **Add**.

Step 6 In the **Profile Name** field of the **Create SXP AP Profiles** slide-in pane, enter a unique name for the profile.

The profile name can contain up to 31 characters. Catalyst Center does not support leading and trailing spaces in the profile name.

Step 7 (Optional) Click the **Status** toggle button to enable the CTS SXP configuration.

Step 8 Enter data in these fields.

- (Optional) **Default Password**: enter a default password for CTS SXP.

  The password can contain up to 80 characters.

- **CTS Listener Minimum (sec)**: enter the minimum CTS SXP listener hold time in seconds.

  The valid range is from 1 to 65534. The default value is 90.

- **CTS Listener Maximum (sec)**: enter the maximum CTS SXP listener hold time in seconds.

  The valid range is from 1 to 65534. The default value is 120.

- **CTS Speaker Seconds (sec)**: enter the CTS SXP speaker hold time in seconds.

  The valid range is from 1 to 65534. The default value is 120.

- **CTS Recon Period (sec)**: enter the CTS SXP reconcile period in seconds.

  The valid range is from 0 to 64000. The default value is 120.

- **CTS Retry Period (sec)**: enter the CTS SXP retry period in seconds.

  The valid range is from 0 to 64000. The default value is 120.

Step 9 (Optional) Under **CTS SXP Profile Connections**, configure CTS SXP profile connections.

If you want to...	Then...
add a CTS SXP profile connection	**a.** Click **Add**. **b.** In the **Peer IP** field of the **Add CTS SXP Profile Connections** dialog box, enter a peer IP address for the SXP connection. **c.** From the **Connection Mode** drop-down list, choose an SXP connection mode. **d.** From the **Password Type** drop-down list, choose a password type for the SXP connection. **e.** Click **Save**.
edit a CTS SXP profile connection	**a.** Check the check box next to the peer IP address that you want to edit. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete CTS SXP profile connections	**a.** Check the check box next to the peer IP addresses that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Configure rogue policies for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure rogue policies to detect rogue APs for a wireless controller and provision them.

The default AP profile and these global rogue parameters are automatically configured for the high, low, or critical rogue detection security levels and you can't edit them:

- **Adhoc Rogue AP**
- **Auto Containment Level**

- **Detect and Report Adhoc Networks**
- **Expiration timeout for Rogue APs (seconds)**
- **Rogue AP Expiration Timeout (sec)**
- **Rogue Auto Contain Ad Hoc**
- **Rogue Init Timer (sec)**
- **Rogue Polling Interval (sec)**
- **Using our SSID**
- **Valid client on Rogue AP**
- **Validate Rogue Clients Against AAA**
- **Validate Rogue APs Against AAA**

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies**.

Step 4 In the **Rogue Policies** tab, under **General**, complete the required configurations.

a) From the **Rogue Detection Security Level** drop-down list, choose a security level.

If you chose the **Custom** security level, complete these configurations.

- In the **Rogue AP Expiration Timeout (sec)** field, enter the timeout value in seconds for rogue APs.

  The valid range is from 240 to 3600. The default value is 1200.

- Use the **Validate Rogue Clients Against AAA** check box to enable or disable the validation of rogue clients against the AAA server.
- Use the **Validate Rogue APs Against AAA** check box to enable or disable validation of rogue APs against the AAA server.
- In the **Rogue Polling Interval (sec)** field, enter the interval to poll the AAA server for rogue information.

  The valid range is from 60 to 86400. The default value is 3600.

- Check the **Detect and Report Adhoc Networks** check box to enable the detection and reporting of ad hoc rogue APs.
- In the **Rogue Init Timer (sec)** field, enter the init timer in seconds for rogue APs.

The valid range is from 0 to 360. The default value is 60.

When a rogue AP is detected, an init timer is started and the rules are applied when this timer expires.

b) In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client per rogue AP SNMP trap.

The valid range is from 0 to 256. The default value is 56.

c) Use the **AP Authentication** check box to enable or disable AP authentication.

Note AP authentication can't be enabled if global MFP is enabled in Step 6, on page 822.

d) In the **AP Authentication Alarm Threshold** field, enter the threshold for AP authentication alarm.

The valid range is from 1 to 255. The default value is 22.

e) Use the **Syslog Notification** check box to enable or disable the rogue event notifications through syslog.

Step 5 If you chose the **Custom** security level, under **Auto Contain**, complete these configurations:

- From the **Auto Containment Level** drop-down list, choose a level for automatic containment of rogue APs.
- Use these check boxes to enable or disable the corresponding configurations:
  - **Auto Containment only for Monitor Mode APs**: Configure auto containment for only the APs that are in monitor mode.
  - **Using our SSID**: Configure auto containment of rogue APs that are advertising our SSID.
  - **Valid client on Rogue AP**: Configure auto containment for valid clients that are using rogue APs.
  - **Adhoc Rogue AP**: Configure auto containment for ad hoc rogue APs.

Step 6 Under **MFP Configuration**, complete these configurations:

- Use the **Global MFP State** check box to enable or disable Management Frame Protection (MFP) globally.

Note Global MFP cannot be enabled if AP authentication is enabled.

- Use the **AP Impersonation Detection** check box to enable or disable AP impersonation detection.
- In the **MFP Key Refresh Interval (hours)** field, enter the MFP key refresh interval in hours.

  The valid range is from 1 to 24.

Step 7 Under **Rogue Device Authorization**, use the **Rogue Authorization Mode** check box to enable or disable the authorization mode for identifying and managing rogue devices on the network.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a rogue AP rule for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies**.

Step 4 Click the **Rogue AP Rules** tab.

Step 5 Click **Add**.

Step 6 In the **Rule Name** field of the **Create Rogue AP Rules** slide-in pane, enter a unique name for the rogue AP rule.

The rule name can contain up to 32 alphanumeric characters and special characters. The rule name must contain at least one alphanumeric character, period (.), underscore (_), or hyphen (-). Catalyst Center does not support ? and spaces in the rule name.

Step 7 In the **Priority** field, enter a number to indicate the priority of the rogue AP rule.

The valid range is from 1 to 512. A lower number indicates a higher priority.

Step 8 From the **Type** drop-down list, choose a classification type.

Step 9 Based on the classification type, complete these configurations.

If you chose...	Then...
Friendly or **Malicious**	From the **State** drop-down list, choose a state for the rogue AP rule.
Custom	• From the **State** drop-down list, choose a state for the rogue AP rule. • In the **Severity Score** field, enter a score for the classification type. The valid range is from 1 to 100. • (Optional) In the **Custom Name** field, enter a custom name for the classification type.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

What to do next

To configure additional parameters for the rule, see Configure a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller, on page 824.

Configure a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure additional parameters for a rogue AP rule for a wireless controller and provision it.

Before you begin

Create rogue AP rules. To create a rogue AP rule, see Create a rogue AP rule for a Cisco Catalyst 9800 Series Wireless Controller, on page 823.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies** > **Rogue AP Rules**.

Step 4 Check the check box for the rule that you want to configure. Hover your cursor over **Actions** and choose **Edit**.

Step 5 (Optional) In the **Priority** field of the **Edit Rogue AP Rules** slide-in pane, update the existing priority of the rogue AP rule.

The valid range is 1 to 512. A lower number indicates a higher priority.

Step 6 Use the **Enable Rule** check box to enable or disable the rule.

Note If you enable the rule, you can edit only the **Priority** field. The other options are disabled.

If you disable the rule, complete these configurations:

a) From the **Type** drop-down list, choose a classification type: **Friendly**, **Malicious**, **Delete**, or **Custom**

Based on the classification type, complete these configurations.

If you chose...	Then...
Friendly or **Malicious**	From the **State** drop-down list, choose a state for the rogue AP rule.
Custom	• From the **State** drop-down list, choose a state for the rogue AP rule. • In the **Severity Score** field, enter a score for the classification type. The valid range is 1 to 100. • (Optional) In the **Custom Name** field, enter a custom name for the classification type. The custom name can contain up to 215 alphanumeric and special characters.

b) From the **Match Operation** drop-down list, choose a criterion for the rogue AP to adopt the classification type of the rule.

- **All**: The detected rogue AP must meet all of the conditions specified in the rule for the rule to be matched.
- **Any**: The detected rogue AP must meet any of the conditions specified in the rule for the rule to be matched.

c) (Optional) Under **Conditions**, check the required check boxes to configure the corresponding conditions to adopt the classification type of the rule:

- **client-count**: This condition requires that a minimum number of clients be associated with the rogue AP.

  If you check this check box, in the **Minimum Number of Rogue Clients** field, enter the minimum number of clients to be associated with the rogue AP. The valid range is 1 to 10. The default value is 0.

  If the number of clients connected exceeds the specified limit, the classification type of the rule is adopted.

- **duration**: This condition requires the rogue AP to be detected for a minimum period of time.

  If you check this check box, in the **Time Duration** field, enter a value for the minimum detection period in seconds. The valid range is 0 to 86400. The default value is 0.

- **encryption**: This condition requires that WLAN uses the specified encryption.

  If you check this check box, you can optionally use the check boxes to choose the corresponding encryption type.

- **infrastructure**: This condition requires that the SSID of the rogue AP must be known to the wireless controller.

  If you check this check box, you can optionally check the **Manage SSID** check box to check if the SSID of the rogue AP matches a managed SSID.

- **rssi**: This condition requires that the rogue AP has a minimum received signal strength indication (RSSI) value.

If you check this check box, in the **Maximum RSSI** field, enter the maximum RSSI value in dBm. The valid range is 0 to –128.

- **channel-width**: This condition requires that the rogue AP uses the channel width for the specified radio band.

  If you check this check box, choose the required option from these drop-down lists:

  - **Band**: Choose the rogue AP radio band.
  - **Maximum Channel Width**: Choose the maximum channel width for the radio band.

- **ssid**: This condition requires that the rogue AP has a specific user-configured SSID.

  If you check this check box, in the **User Configured SSID** field, enter the SSIDs. You can enter one SSID per line.

- **substring-ssid**: This condition requires that the rogue AP has a substring of the specific user-configured SSID. The wireless controller analyzes the occurrence pattern and identifies a match if the substring is found in the SSID string.

  If you check this check box, in the **User Configured Substring-SSID** field, enter the substring of SSIDs. You can enter one substring of the SSID per line.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure client exclusion policies for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure client exclusion policies for a wireless controller and provision.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **Wireless Protection Policies**.

Step 4 Click the **Client Exclusion Policies** tab.

Step 5 (Optional) Check the required check boxes to exclude clients for the corresponding events.

- **Select All Events**: choose all the events for client exclusion.
- **Excessive 802.11 Association Failures**: exclude clients when there are repeated 802.11 association failures.
- **Excessive 802.1X Authentication Failures**: exclude clients when there are repeated 802.1X authentication failures.
- **Excessive 802.11 Authentication Timeout**: exclude clients when there are repeated 802.11 authentication timeouts.
- **IP Theft or IP Reuse**: exclude clients when they reuse an IP address indicating a possible IP theft.
- **Excessive Web Authentication Failures**: exclude clients when there are repeated web authentication failures.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure LSC provision parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the parameters for AP Locally Significant Certificate (LSC) provisioning for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **LSC**.

Step 4 Go to the **LSC Provision** tab and under **Provisioning Configuration**, configure the AP join attempts with LSC:

- From the **Status** drop-down list, choose a status for LSC provisioning.

  When you enable the status, APs can use LSC provisioning. When you disable the status, APs fall back to Manufacturer Installed Certificate (MIC) or Self-Signed Certificate (SSC).

- (Optional) In the **Trustpoint Name** field, enter the trustpoint for the Certificate Authority (CA) server that provides certificates to APs and wireless controller for LSC provisioning.
- (Optional) In the **Number of Join Attempts** field, enter the number of join attempts an AP makes using LSC before falling back to MIC.

  The valid range is from 0 to 255.
- From the **Key Size** drop-down list, choose the size of the keys used for LSC provisioning.

Step 5 (Optional) Under **Subject Name Parameters**, enter the required parameters that are included in the certificate-signing request sent from APs.

Configure the required country, state, city, department, organization, and email address.

Step 6 (Optional) Under **LSC Renewal Configuration**, use the **LSC Auto-Renewal** check box, to enable or disable renewal of LSC during AP join.

If you enable LSC renewal during AP join, complete these configurations:

- In the **Due Time (Days)** field, enter the number of days before the LSC expires to initiate renewal.

  The valid range is from 5 to 365.
- (Optional) From the **Renewal Schedule** drop-down list, choose a calendar profile.

  To create a calendar profile, see Create a calendar profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 759.
- Use the **Syslog** toggle button to enable or disable periodic syslog messages for LSC renewal.
- From the **Renewal Mode** drop-down list, choose a renewal mode.
  - **One Shot**: renew certificates for all applicable APs at once.
  - **Staggered**: renew certificates for applicable APs in batches.

If you choose staggered renewal, complete these configurations under **Staggered Renewal Configuration**:



Note To configure AP upgrade settings, see Configure AP upgrade settings for a Cisco Catalyst 9800 Series Wireless Controller, on page 968.

- From the **Accounting Action** drop-down list, choose an action to be taken when APs are missing during accounting.
- (Optional) In the **Accounting Percent** field, enter the percentage of APs that must join back during accounting.

  The valid range is from 0 to 100.
- In the **Iteration Expiry (Minutes)** field, enter the time in minutes after which the staggered iteration expires for LSC provisioning on the AP.

  The valid range is from 0 to 255.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create an LSC provisioning entry for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Locally Significant Certificate (LSC) provisioning entry for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **LSC**.

Step 4 Click the **LSC Provisioning Entries** tab.

Step 5 Hover your cursor over **Add** and choose the required option:

- **Add Single AP MAC**: Configure a single MAC address for LSC provisioning entry.
- **Add Multiple AP MACs(Upload CSV)**: Upload a comma-separated value (CSV) file to configure multiple MAC addresses for LSC provisioning entries.

If you choose...	Then...
Add Single AP MAC	in the **AP MAC Address** field of the **Create LSC Provisioning Entries** slide-in pane, enter the AP Ethernet MAC address to which the LSC will be provisioned. Enter the MAC address in xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, xxxx-xxxx-xxxx, or xxxx:xxxx:xxxx format.

If you choose...	Then...
Add Multiple AP MACs(Upload CSV)	**a.** Click **sample CSV** to download the sample CSV file. **b.** Enter the MAC addresses to which the LSC will be provisioned in the CSV file. Enter MAC addresses in xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, xxxx-xxxx-xxxx, or xxxx:xxxx:xxxx format. **c.** Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**. **d.** Click **Upload**. Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create a key chain for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a key chain for a wireless controller running Cisco IOS XE Release 26.1.1 or later and provision it.

Key chains are used to group authentication keys for secure communication protocols such as routing authentication.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **MACsec Key Chain**.

Step 4 Click **Add**.

Step 5 In the **Create Key Chain Configuration** slide-in pane, complete these configurations.

a) In the **Key Chain Name** field, enter a unique name for the key chain.

b) Configure key chains.

If you want to...	Then...
add a key chain	1. Click **Add**. 2. In the **Key ID** field of the **Add Key Chain** dialog box, enter a key identifier. For a regular key chain, enter a number from 0 to 2147483674. For a Media Access Control security (MACsec) key chain, enter a hexadecimal number that contains an even number of digits. 3. (Optional) From the **MACsec Cryptographic Algorithm** drop-down list, choose an algorithm for MACsec. 4. (Optional) In the **Key String** field, enter the hexadecimal key string for authentication or encryption. For AES 128-bit Cipher-based Message Authentication Code (CMAC), enter a 32-character string in this field. For AES 256-bit CMAC, enter a 64-character string in this field. 5. (Optional) From the **Key String Encryption Type** drop-down list, choose an encryption method for storing the key string. 6. Click **Save**.
edit a key chain	1. Check the check box for the key chain that you want to edit. 2. Hover your cursor over **Actions** and choose **Edit**. 3. Edit the required configurations. 4. Click **Save**.
delete a key chain	1. Check the check box for the key chain that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure AP certificate policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure AP certificate policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AP Certificate Policy**.

Step 4 Use the **Allow MIC APs** toggle button to enable or disable the usage of Manufacturer Installed Certificates (MIC) for APs to join the wireless controller.

Step 5 (Optional) From the **Trustpoint Name for MIC APs** drop-down list, select a trustpoint to specify the certificate authority and secure communication for the wireless management interface.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an AP certificate policy using MAC address for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP certificate policy for a wireless controller using MAC address and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AP Certificate Policy**.

Step 4 Hover your cursor over **MAC/Serial Number** and choose **MAC**.

Step 5 Hover your cursor over **Add** and choose the required method.

- **Add Single Entry**: Creates AP certificate policy using a single MAC address.
- **Upload CSV**: Creates AP certificate policy using MAC addresses listed in a comma-separated value (CSV) file.

If you choose...	Then...
Add Single Entry	In the **AP Ethernet MAC Address** field of the **Create AP Certificate Policy MAC** slide-in pane, enter the Ethernet MAC address of the AP to which this policy applies. Enter the MAC address in the format xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, or xx:xx:xx:xx:xx:xx.
Upload CSV	In the **Upload CSV** slide-in pane, complete these configurations: **a.** Click **sample CSV** to download the sample CSV file. **b.** Enter the Ethernet MAC addresses of the AP to which this policy applies. Enter the MAC addresses in the format xxxx.xxxx.xxxx, xx-xx-xx-xx-xx-xx, or xx:xx:xx:xx:xx:xx. **c.** Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**. **d.** Click **Upload**. Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an AP certificate policy using serial number for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an AP certificate policy for a wireless controller using serial number and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Security** and click **AP Certificate Policy**.

Step 4 Hover your cursor over **MAC/Serial Number** and choose **Serial Number**.

Step 5 Hover your cursor over **Add** and choose the required method.

- **Add Single Entry**: Creates AP certificate policy using a single serial number.
- **Upload CSV**: Creates AP certificate policy using serial numbers listed in a comma-separated value (CSV) file.

If you choose...	Then...
Add Single Entry	In the **Trust Anchor Serial Number** field of the **Create AP Certificate Policy Serial Number** slide-in pane, enter the serial number of the trust anchor certificate associated with the AP. The serial number must contain 11 numeric characters. **Note** Ensure that the serial number matches the serial number issued by the certificate authority.

If you choose...	Then...
Upload CSV	In the **Upload CSV** slide-in pane, complete these configurations: **a.** Click **sample CSV** to download the sample CSV file. **b.** Enter the serial numbers of the trust anchor certificate associated with the AP. The serial number must contain 11 numeric characters. **Note** Ensure that the serial number matches the serial number issued by the certificate authority. **c.** Either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**. **d.** Click **Upload**. Catalyst Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message is displayed.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device global wireless configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Configure CleanAir for a Cisco Catalyst 9800 Series Wireless Controller

Cisco CleanAir technology uses silicon-level intelligence to create a spectrum-aware, self-healing, and self-optimizing wireless network that mitigates the impact of wireless interference.

Use this procedure to configure the CleanAir parameters for a wireless controller and provision.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **CleanAir**.

Step 4 In the **6 GHz** tab, complete these configurations.

a) Use the **Enable CleanAir** toggle button to enable or disable CleanAir on the 6-GHz band.
b) Use the **Report Interferers** check box to enable or disable the reporting of interferers.
c) Under **Trap Configuration**, complete these configurations.

- (Optional) Check the **Enable Air Quality Index (AQI) Trap** check box to enable air quality notification on this band.
- In the **AQI Alarm Threshold** field, enter the threshold value for the AQI trap.

  The valid range is from 1 to 100. The default value is 10.
- Check the **Enable Interference for Security Alarm** check box to enable Interference Device Reports (IDR) notification on this band.

d) Under **Advanced CleanAir Configuration**, complete these configurations:

- Use the **Air Quality Alarm for Unclassified category** toggle button to enable or disable the air quality alarm for the unclassified category.
- (Optional) In the **Air Quality Alarm Threshold for Unclassified category** field, enter the threshold value for air quality alarm for unclassified category.

  The valid range is from 1 to 100.

e) Under **Interference Types to Detect** and **Interference Types to Trap**, check the required check boxes to choose the corresponding interference types.
f) Complete Step 7, on page 837 to Step 10, on page 838 to provision the configuration.

Step 5 In the **5 GHz** tab, complete these configurations.

a) Use the **Enable CleanAir** toggle button to enable or disable CleanAir on the 5-GHz band.
b) (Optional) Check the **Enable Spectrum Intelligence (SI)** check box to enable spectrum intelligence (SI) on this band.
c) (Optional) Check the **Report Interferers** check box to enable the reporting of interferers.
d) Under **Trap Configuration**, complete these configurations.

- (Optional) Check the **Enable Air Quality Index (AQI) Trap** check box to enable air quality notification on this band.
- In the **AQI Alarm Threshold** field, enter the threshold value for the AQI trap.

The valid range is from 1 to 100. The default value is 10.

- Check the **Enable Interference for Security Alarm** check box to enable IDR notification on this band.

e) Under **Advanced CleanAir Configuration**, complete these configurations:

- Use the **Air Quality Alarm for Unclassified category** toggle button to enable or disable the air quality alarm for the unclassified category.
- (Optional) In the **Air Quality Alarm Threshold for Unclassified category** field, enter the threshold value for air quality alarm for unclassified category.

  The valid range is from 1 to 100.

f) Under **Interference Types to Detect** and **Interference Types to Trap**, check the required check boxes to choose the corresponding interference types.

g) Complete Step 7, on page 837 to Step 10, on page 838 to provision the configuration.

Step 6 In the **2.4 GHz** tab, complete these configurations.

a) Use the **Enable CleanAir** toggle button to enable or disable CleanAir on the 2.4-GHz band.

b) (Optional) Check the **Enable Spectrum Intelligence (SI)** check box to enable spectrum intelligence (SI) on this band.

c) Check the **Report Interferers** check box to enable the reporting of interferers.

d) Under **Trap Configuration**, complete these configurations.

- Check the **Enable Air Quality Index (AQI) Trap** check box to enable air quality notification on this band.
- In the **AQI Alarm Threshold** field, enter the threshold value for the AQI trap.

  The valid range is from 1 to 100. The default value is 10.

- Check the **Enable Interference for Security Alarm** check box to enable IDR notification on this band.

e) Under **Advanced CleanAir Configuration**, complete these configurations:

- Use the **Air Quality Alarm for Unclassified category** toggle button to enable or disable the air quality alarm for the unclassified category.
- (Optional) In the **Air Quality Alarm Threshold for Unclassified category** field, enter the threshold value for air quality alarm for the unclassified category.

  The valid range is from 1 to 100.

f) Under **Interference Types to Detect** and **Interference Types to Trap**, check the required check boxes to choose the corresponding interference types.

g) Complete Step 7, on page 837 to Step 10, on page 838 to provision the configuration.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure high throughput parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the high throughput parameters for a wireless controller and provision the configuration.

Important Configuring high throughput on operational bands results in loss of client connectivity.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **High Throughput**.

Step 4 In the **6 GHz** tab, configure the high throughput parameters for the 6-GHz band.

a) (Optional) Under **11ax**, complete these configurations:

- Under **SS/MCS**, check the required check boxes to choose the corresponding Spatial Streams (SS) or modulation and coding scheme (MCS) configurations.
- From the **Beamforming Support** drop-down list, choose a status to enable or disable beamforming for the WLAN.

  Beamforming improves signal quality and range by directing signals towards connected clients.
- Use the **HE Dynamic Fragmentation** toggle button to enable or disable dynamic fragmentation for high efficiency (HE) 802.11ax transmissions.

b) (Optional) Under **11be**, complete these configurations.

- Use the **Enable 11be** toggle button to enable or disable the wireless controller to manage the 802.11be networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.

c) Complete Step 7, on page 840 to Step 10, on page 841 to provision the configuration.

Step 5 In the **5 GHz** tab, configure the high throughput parameters for the 5-GHz band.

a) (Optional) Under **11n**, complete these configurations.

- Use the **Enable 11n** toggle button to enable or disable the wireless controller to manage the 802.11n networks.
- Use the **Dot11n Short Guard Enabled** toggle button to enable or disable the support for 802.11n guard interval on this band.
- Under **MCS/(Data Rate)**, check the required check boxes to choose the corresponding MCS or data rate configurations.

b) (Optional) Under **11ac**, complete these configurations.

- Use the **Enable 11ac** toggle button to enable or disable the wireless controller to manage the 802.11ac networks.
- Under **SS/MCS/(Data Rate)**, check the required check boxes to choose the corresponding SS or MCS or data rate configurations.

c) (Optional) Under **11ax**, complete these configurations.

- Use the **Enable 11ax** toggle button to enable or disable the wireless controller to manage the 802.11ax networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.
- From the **Beamforming Support** drop-down list, choose a status to enable or disable beamforming for the WLAN.

  Beamforming improves signal quality and range by directing signals towards connected clients.
- Use the **RIFS Transmission Status** toggle button to enable or disable the usage of Reduced Interframe Spacing (RIFS) for transmissions.
- Use the **HE Dynamic Fragmentation** toggle button to enable or disable dynamic fragmentation for high efficiency (HE) 802.11ax transmissions.

d) (Optional) Under **11be**, complete these configurations.

- Use the **Enable 11be** toggle button to enable or disable the wireless controller to manage the 802.11be networks.

- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.

e) Complete Step 7, on page 840 to Step 10, on page 841 to provision the configuration.

Step 6 In the **2.4 GHz** tab, configure the high throughput parameters for the 2.4-GHz band.

a) (Optional) Under **11n**, complete these configurations.

- Use the **Enable 11n** toggle button to enable or disable the wireless controller to manage the 802.11n networks.
- Use the **Dot11n Short Guard Enabled** toggle button to enable or disable the support for 802.11n guard interval on this band.
- Under **MCS/(Data Rate)**, check the required check boxes to choose the corresponding MCS or data rate configurations.

b) (Optional) Under **11ax**, complete these configurations.

- Use the **Enable 11ax** toggle button to enable or disable the wireless controller to manage the 802.11ax networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.
- From the **Beamforming Support** drop-down list, choose a status to enable or disable beamforming for the WLAN.

  Beamforming improves signal quality and range by directing signals towards connected clients.
- Use the **RIFS Transmission Status** toggle button to enable or disable the usage of Reduced Interframe Spacing (RIFS) for transmissions.
- Use the **HE Dynamic Fragmentation** toggle button to enable or disable dynamic fragmentation for high efficiency (HE) 802.11ax transmissions.

c) (Optional) Under **11be**, complete these configurations.

- Use the **Enable 11be** toggle button to enable or disable the wireless controller to manage the 802.11be networks.
- Under **SS/MCS**, check the required check boxes to choose the corresponding SS or MCS configurations.

d) Complete Step 7, on page 840 to Step 10, on page 841 to provision the configuration.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).

Option	Description
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure media parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the video and voice media parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Media Parameters**.

Step 4 Hover your cursor over **6 GHz**, **5 GHz**, or **2.4 GHz**, click **Media**, and configure the required parameters.

a) (Optional) Under **Media**, check the **Unicast Video Redirect** check box to redirect a unicast or multicast only video stream on a best-effort basis.
b) (Optional) Under **Multicast Direct Admission Control**, complete these configurations.
   - Check the **Media Stream Admission Control (ACM)** check box to enable admission control for the video access category.
   - Enter data in these fields.
     - **Maximum Media Streams RF Bandwidth (%)**: enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band.

       The valid range is from 5 to 85. The default value is 5.
     - **Maximum Media Bandwidth (%)**: enter the percentage of the maximum allowed bandwidth for media traffic.

The valid range is from 5 to 85. The default value is 85.

- From the **Client Minimum Phy Rate (kbps)** drop-down list, choose a minimum client rate for multicast direct streams.
- In the **Maximum Retry Percentage (%)** field, enter the maximum retry percentage for multicast direct streams.

  The valid range is from 0 to 100. The default value is 80.

c) (Optional) Under **Media Stream - Multicast Direct**, configure the required parameters.

- Check the required check boxes to configure the corresponding settings.
  - **Enable Multicast Direct**: allow multicast direct stream on radio
  - **Best Effort QoS Admission**: admit a media stream in a best-effort queue
- Enter data in these fields.
  - **Maximum Stream Per Radio**: choose the maximum number of allowed media streams per radio.
  - **Maximum Stream Per Client**: choose a maximum number of allowed media streams per client.

d) (Optional) Under **Call Admission Control (CAC) Advanced**, complete these configurations:

- For the 5-GHz band, in **Default 802.11a/n QoS Packet Maximum (bytes)** field, enter the maximum allowed packet size in bytes for QoS on 802.11a/n networks.

  The valid range is from 15000 to 400000000.
- In the **CAC Maximum Concurrent Calls** field, enter the maximum number of simultaneous voice or video calls allowed on the AP or radio band.

  The valid range is from 0 to 4294967295. If you do not want to configure a limit, leave this field blank.

e) Complete Step 6, on page 843 to Step 9, on page 844 to provision the configuration.

Step 5 Hover your cursor over **6 GHz**, **5 GHz**, or **2.4 GHz**, click **Voice**, and configure the required voice parameters.

a) (Optional) Under **Voice**, check the **Call Admission Control (ACM)** check box to enable admission control on the voice access category.

If you check this check box, complete these configurations.

- Check the **Load-Based CAC** check box to enable load-based Channel Availability Check (CAC).
- Enter data in these fields.
  - **Maximum RF bandwidth (%)**: enter the percentage of maximum bandwidth allocated to the 802.11e clients.

    The valid range is from 5 to 85. The default value is 75.
  - **Reserved Roaming Bandwidth (%)**: enter the percentage of maximum bandwidth allocated to roaming clients for voice traffic.

    The valid range is from 0 to 25. The default value is 6.
- Check the **Expedited Bandwidth** check box to enable the expedited bandwidth request support.

- Under **SIP CAC and Bandwidth**, check the **SIP CAC Support** check box to enable SIP CAC support.

  If you enable SIP CAC support, complete the required configurations.

  - In the **SIP Bandwidth (kbps)** field, enter the bandwidth in kbps for the SIP CAC configuration of the dot11 band for the APs associated with this controller.

    The valid range is from 8 to 64. The default value is 64.

  - From the **SIP Voice Sample Interval (ms)** drop-down list, choose a voice sample interval in milliseconds for the SIP CAC configuration of the dot11 band for the APs associated with this controller.

b) (Optional) Under **Traffic Stream Metrics**, complete the required configurations.

- Check the required check boxes to enable the corresponding configurations.
  - **Metrics Collection**: enable the 802.11a traffic stream metrics support.

    When you enable the metrics, the associated APs send the controller statistical data on the traffic on their 802.11a interfaces every 90 seconds.

  - **Inactivity Timeout**: enable the Traffic Specification (TSPEC) inactivity timeout processing mode.

- Enter data in these fields.
  - **Stream Size**: enter the maximum acceptable data rate of the media stream.

    The valid range is from 84000 to 92100.

  - **Maximum Streams**: enter the maximum number of media streams per TSPEC.

    The valid range is from 1 to 5.

c) Complete Step 6, on page 843 to Step 9, on page 844 to provision the configuration.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure Air Time Fairness for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the Air Time Fairness (ATF) parameters for a wireless controller.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand c and click **Airtime Fairness**.

Step 4 Click either the **5 GHz** or **2.4 GHz** tab and complete these configurations.

a) Use the **Status** toggle button to enable or disable ATF on the band.
b) From the **Mode** drop-down list, choose an ATF operating mode.

If you chose the **Enforced** mode, you can optionally check the **Optimization** check box to enable the ATF optimization.

c) Check the **Bridge Client Access** check box to enable the air time allocation mode on the default RF policy.

If you check the **Bridge Client Access** check box, in the **Airtime Allocation** field, you can optionally enter an air time allocation weight percentage.

The valid range is from 5 to 90. The default value is 5.

Step 5 Click **Review and Provision**.

Step 6 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Option	Description
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an Air Time Fairness policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an Air Time Fairness (ATF) policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Airtime Fairness**.

Step 4 Click the **Policy** tab.

Step 5 Click **Add**.

Step 6 In the **ATF Policy Name** field of the **Create ATF Policy** slide-in pane, enter a unique name for the ATF policy.

Step 7 In the **ID** field, enter a unique ID for the ATF policy.

The valid range is from 0 to 511.

Step 8 In the **Weight** field, enter a policy weight for the ATF policy.

The valid range is from 5 to 100. The default value is 10.

Step 9 (Optional) Check the **Client Sharing** check box to enable fair client sharing for an ATF policy.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Configure network parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the network parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Network Parameters**.

Step 4 In the **6 GHz** tab, configure the required parameters for the 6-GHz band.

a) Under **General**, complete these configurations.

- (Optional) Check the **6 GHz Network Status** check box to enable the 6-GHz band.

Note When this band is operational, configuring **Beacon Interval (msec)**, **Fragmentation Threshold (bytes)**, or **DTPC Support** results in loss of connectivity for clients.

- Enter data in these fields.
  - **Beacon Interval (msec)**: enter the time in milliseconds that an AP radio can use for scheduling beacon transmissions.

    The valid range is from 20 to 1000. The default value is 100.
  - **Fragmentation Threshold (bytes)**: enter the size in bytes at which the packets are fragmented.

    The valid range is from 256 to 2346. The default value is 2346.

- (Optional) Check the **DTPC Support** check box to enable Dynamic Transmit Power Control (DTPC) on all 802.11b/g bands.

  When DTPC is enabled, the radios advertise their transmit power levels in beacons and probe responses.

Note If you enable DTPC, you can't configure a power constraint value for the 5-GHz band. For more information, see Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 851.

b) (Optional) Under **CCX Location Measurement**, check the **Mode** check box to enable the support for 802.11 Cisco Client Extensions (CCX) client location measurements.

If you enable this measurement, in the **Interval** field, enter the 802.11 CCX client location measurement interval.

The valid range for this interval is from 10 to 32400. The default value is 60.

c) (Optional) Under **A-MPDU Tx** and **A-MSDU Tx**, choose the required priority levels for which you want to enable the Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU) transmission priority.

d) Under **General 802.11 Parameters**, use the **Enable World Mode (IE)** toggle button to enable or disable the inclusion of world mode information element (IE) in beacon frames for APs.

Enable this option if you network serves clients from different regulatory domains or to ensure compliance with international wireless standards.

e) Complete Step 7, on page 850 to Step 10, on page 851 to provision the configuration.

Step 5 In the **5 GHz** tab, configure the required parameters for the 5-GHz band.

a) Under **General**, complete these configurations.

- (Optional) Check the **5 GHz Network Status** check box to enable the 5-GHz band.

Note When this band is operational, configuring **Beacon Interval (msec)**, **Fragmentation Threshold (bytes)**, **DTPC Support**, or data rates results in loss of connectivity for clients.

- Enter data in these fields.
  - **Beacon Interval (msec)**: enter the time in milliseconds that an AP radio can use for scheduling beacon transmissions.

    The valid range is from 20 to 1000. The default value is 100.
  - **Fragmentation Threshold (bytes)**: enter the size in bytes at which the packets are fragmented.

    The valid range is from 256 to 2346. The default value is 2346.
  - **RSSI Threshold (dBm)**: enter the minimum RSSI threshold for optimized roaming to occur.

    The valid range is from -127 to 0. The default value is -127.
- (Optional) Check the required check boxes to configure the required settings.
  - **DTPC Support**: enable DTPC on all 802.11b/g bands.

    When DTPC is enabled, the radios advertise their transmit power levels in beacons and probe responses.

Note If you enable DTPC, you can't configure a power constraint value for the 5-GHz band. For more information, see Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 851.

  - **Tri Radio Mode**: enable the tri-radio mode.
  - **RSSI Low Check**: check if the RSSI threshold is enabled before optimized roaming occurs.

b) (Optional) Under **CCX Location Measurement**, check the **Mode** check box to enable the support for 802.11 CCX client location measurements.

If you enable this measurement, in the **Interval** field, enter the 802.11 CCX client location measurement interval.

The valid range for this interval is from 10 to 32400. The default value is 60.

c) Under **Data Rates**, from the data rate drop-down lists, choose the required options for the corresponding data rates.

Option	Description
Mandatory	Clients must support this data rate to associate to an AP with the wireless controller.
Supported	Any associated clients that support this data rate may communicate with the AP using that rate.
Disabled	Clients specify the data rates used for communication.

d) (Optional) Under **A-MPDU Tx**, complete these configurations:

- In the **Ampdu Window Size** field, enter the window size for A-MPDU.

  The valid range is from 1 to 255.

- Use the **Aggregation Scheduler** toggle button to enable or disable the 802.11n A-MPDU scheduler.
- From the **Frame Burst** drop-down list, choose the required settings for bursting of 802.11n A-MPDUs.
- In the **Realtime Traffic Timeout** field, enter the A-MPDU transmit aggregation scheduler real-time traffic timeout in milli seconds.

  The valid range is from 1 to 1000.

- Choose the required priority levels for which you want to enable the A-MSDU transmission priority.

e) (Optional) Under **A-MSDU Tx**, choose the required priority levels for which you want to enable the A-MSDU transmission priority.

f) Under **General 802.11 Parameters**, use the **Enable World Mode (IE)** toggle button to enable or disable the inclusion of world mode information element (IE) in beacon frames for APs.

Enable this option if you network serves clients from different regulatory domains or to ensure compliance with international wireless standards.

g) Complete Step 7, on page 850 to Step 10, on page 851 to provision the configuration.

Step 6 In the **2.4 GHz** tab, configure the required parameters for the 2.4-GHz band.

a) Under **General**, complete these configurations.

- (Optional) Check the **2.4 GHz Network Status** check box to enable the 2.4-GHz band.

Note When this band is operational, configuring **802.11g Network Status**, **Beacon Interval (msec)**, **Short Preamble**, **Fragmentation Threshold (bytes)**, **DTPC Support**, or data rates results in loss of connectivity for clients.

- Use the **802.11g Network Status** toggle button to enable or disable 802.11g support on the 802.11b network.
- Enter data in these fields.
  - **Beacon Interval (msec)**: enter the time in milliseconds that an AP radio can use for scheduling beacon transmissions.

    The valid range is from 20 to 1000. The default value is 100.

  - **Fragmentation Threshold (bytes)**: enter the size in bytes at which the packets are fragmented.

    The valid range is from 256 to 2346. The default value is 2346.

  - **RSSI Threshold (dBm)**: enter the minimum RSSI threshold for optimized roaming.

    The valid range is from -127 to 0. The default value is -127.

- Check the required check boxes to configure the corresponding settings.
  - **Short Preamble**: enable transmission of the short version of the radio preamble.

- **DTPC Support**: enable DTPC on all 802.11b/g bands.

  When DTPC is enabled, the radios advertise their transmit power levels in beacons and probe responses.

Note If you enable DTPC, you can't configure a power constraint value for the 5-GHz band. For more information, see Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller, on page 851.

- **RSSI Low Check**: check if the RSSI threshold is enabled before optimized roaming occurs.

b) (Optional) Under **CCX Location Measurement**, check the **Mode** check box to enable the support for 802.11 CCX client location measurements.

If you enable this measurement, in the **Interval** field, enter the 802.11 CCX client location measurement interval.

The valid range for this interval is from 10 to 32400. The default value is 60.

c) Under **Data Rates**, from the data rate drop-down lists, choose the required options for the corresponding data rates.

Option	Description
Mandatory	Clients must support this data rate to associate to an AP with the wireless controller.
Supported	Any associated clients that support this data rate may communicate with the AP using that rate.
Disabled	Clients specify the data rates used for communication.

d) (Optional) Under **A-MPDU Tx**, complete these configurations:

- In the **Ampdu Window Size** field, enter the window size for A-MPDU.

  The valid range is from 1 to 255.

- Use the **Aggregation Scheduler** toggle button to enable or disable the 802.11n A-MPDU scheduler.
- In the **Realtime Traffic Timeout** field, enter the A-MPDU transmit aggregation scheduler real-time traffic timeout in milli seconds.

  The valid range is from 1 to 1000.

- Choose the required priority levels for which you want to enable the A-MSDU transmission priority.

e) (Optional) Under **A-MSDU Tx**, choose the required priority levels for which you want to enable the A-MSDU transmission priority.

f) Under **General 802.11 Parameters**, use the **Enable World Mode (IE)** toggle button to enable or disable the inclusion of world mode information element (IE) in beacon frames for APs.

Enable this option if you network serves clients from different regulatory domains or to ensure compliance with international wireless standards.

g) Complete Step 7, on page 850 to Step 10, on page 851 to provision the configuration.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure global radio parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global radio parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Global Parameters**.

Step 4 In the **6 GHz** tab, configure the required parameters for the 6-GHz band.

a) Under **EDCA**, complete these configurations.

Note When this band is operational, configuring an Enhanced Distributed Channel Access (EDCA) profile or DFS channel switch announcement mode results in loss of connectivity for clients.

- From the **EDCA Profile** drop-down list, choose an EDCA profile for usage in the EDCA parameter set element.

  EDCA parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

- (Optional) Check the **Client Load Based Configuration** check box to enable the client load-based EDCA and reduce collisions by dynamically changing EDCA parameters of clients based on the active client and load.

b) Under **802.11ax**, check the required check boxes to enable the required configurations.

- **Target Wake Up Time**: enable an AP to manage activity in the Wi-Fi network.

  The AP manages activity by

  - minimizing medium contention between Stations (STAs), and
  - reducing the required amount of time that an STA in the power-save mode needs to be awake.

- **Multiple BSSID**: enable 802.11ax the multiple basic service set identifier (BSSID) functionality.
- **Target Wake up time broadcast**: enable broadcasting of 802.11ax target wake-up time.
- **BSS Color**: enable 802.11ax BSS color functionality.

c) Complete Step 7, on page 854 to Step 10, on page 855 to provision the configuration.

Step 5 In the **5 GHz** tab, configure the required parameters for the 5-GHz band.

a) Under **EDCA**, complete these configurations.

Note When this band is operational, configuring the EDCA profile, DFS channel switch announcement mode, or Overlapping BSS Packet Detect (OBSS-PD) results in loss of connectivity for clients.

- From the **EDCA Profile** drop-down list, choose an EDCA profile for usage in the EDCA parameter set element.

  EDCA parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

- (Optional) Check the **Client Load Based Configuration** check box to enable the client load-based EDCA and reduce collisions by dynamically changing EDCA parameters of clients based on the active client and load.

b) Under **802.11ax**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Target Wake Up Time**: enable an AP to manage activity in the Wi-Fi network.

    The AP manages activity by

- minimizing medium contention between Stations (STAs), and
- reducing the required amount of time that an STA in the power-save mode needs to be awake.

- **BSS Color**: enable 802.11ax BSS color functionality.
- **Target Wake up time broadcast**: enable broadcasting of 802.11ax target wake-up time.
- **OBSS PD**: enable OBSS-PD spatial reuse.

- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter the non-Spatial Reuse Group (SRG) OBSS PD maximum threshold in dBm.

  The valid range is from -82 to -62.
- (Optional) Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
- Enter data in these fields.
  - **SRG OBSS PD Min Threshold (dBm)**: enter the SRG OBSS-PD minimum threshold in dBm.

    The valid range is from -82 to -62.
  - **SRG OBSS PD Max Threshold (dBm)**: enter the SRG OBSS-PD maximum threshold in dBm.

    The valid range is from -82 to -62.

c) Under **DFS (802.11h)**, complete these configurations.

- Check the **Channel Switch Status** check box to enable the channel switch functionality.
- Check the **Smart DFS** check box to enable Dynamic Frequency Selection (DFS) and avoid interference with the radar signals.
- From the **Channel Switch Announcement Mode** drop-down list, choose a mode.
- In the **Power Constraint** field, enter the power constraint value.

  The valid range is from 0 to 30.

d) Complete Step 7, on page 854 to Step 10, on page 855 to provision the configuration.

Step 6 In the **2.4 GHz** tab, configure the required parameters for the 2.4-GHz band.

a) Under **EDCA**, complete these configurations.



Note When this band is operational, configuring the EDCA profile or OBSS-PD results in loss of connectivity for clients.

- From the **EDCA Profile** drop-down list, choose an EDCA profile for usage in the EDCA parameter set element.

  EDCA parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.
- (Optional) Check the **Client Load Based Configuration** check box to enable the client load-based EDCA and reduce collisions by dynamically changing EDCA parameters of clients based on the active client and load.

b) Under **802.11ax**, complete these configurations.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Target Wake Up Time**: enable an AP to manage activity in the Wi-Fi network.

    The AP manages activity by
    - minimizing medium contention between Stations (STAs), and
    - reducing the required amount of time that an STA in the power-save mode needs to be awake.
  - **BSS Color**: enable 802.11ax BSS color functionality.
  - **Target Wake up time broadcast**: enable broadcasting of 802.11ax target wake-up time.
  - **OBSS PD**: enable OBSS-PD spatial reuse.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter the non-SRG OBSS PD maximum threshold in dBm.

  The valid range is from -82 to -62.
- (Optional) Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
- Enter data in these fields.
  - **SRG OBSS PD Min Threshold (dBm)**: enter the SRG OBSS-PD minimum threshold in dBm.

    The valid range is from -82 to -62.
  - **SRG OBSS PD Max Threshold (dBm)**: enter the SRG OBSS-PD maximum threshold in dBm.

    The valid range is from -82 to -62.

c) Complete Step 7, on page 854 to Step 10, on page 855 to provision the configuration.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure RRM on the 6-GHz band for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the Radio Resource Management (RRM) parameters on the 6-GHz band for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

Step 4 Hover your cursor over **6 GHz**, choose **General**, and complete these configurations.

a) Under **Profile Threshold for Traps**, complete these configurations.

- In the **Throughput (Bps)** field, enter the 802.11a throughput threshold.

  The valid range is from 1000 to 10000000. The default value is 1000000.

- (Optional) Check the **Automatic CFG** check box to enable the performance profile mode.

b) Under **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels**, from the drop-down lists, choose the required options.

Note CleanAir and SI monitoring is performed only when the AP is in monitor mode.

- **Channel List**: choose the channel for monitoring.
- **RRM Neighbor Discover Type**: choose a mode for the Neighbor Discovery Protocol (NDP).

c) Under **Monitor Intervals**, complete these configurations.

- Enter data in these fields.

- **Neighbor Packet Frequency (sec)**: enter the interval in seconds to specify the frequency of receiving new signal strength, noise, and interference measurements at each AP.

  The valid range is from 60 to 3600. The default value is 180.

- **Reporting Interval (sec)**: enter the interval in seconds between each measurement report.

  The valid range is from 60 to 3600. The default value is 180.

- **Neighbor Timeout Factor**: enter the neighbor timeout factor to specify the duration after which the neighbor expires if it doesn't receive its neighbor packets.

  The valid range is from 5 to 60. The default value is 20.

- **Monitor Coverage Interval**: enter the interval in seconds to receive the new coverage measurements at each AP.

  The valid range is from 60 to 3600.

- **Monitor Load Interval**: enter the interval in seconds to receive the new load measurements at each AP.

  The valid range is from 60 to 3600.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Channel Monitor Status**: enable the neighbor monitoring mode
  - **Monitor RSSI Normalization**: enable 802.11 neighbor discovery RSSI normalization
  - **Sys Log Load**: enable the logging mode for the load profile
  - **Sys Log Channel**: enable logging mode for the dynamic channel change
  - **Sys Log Performance**: enable logging mode for the performance profile
  - **Sys Log Coverage**: enable logging mode for the coverage profile
  - **Sys Log Foreign**: enable logging mode for the foreign profile

- Use the **Log Noise Events** toggle button to log noise-related events detected by the RRM system.

  Logging noise events helps in monitoring and troubleshooting wireless interference issues.

d) Complete Step 10, on page 859 to Step 13, on page 859 to provision the configuration.

Step 5 Hover your cursor over **6 GHz**, choose **Coverage**, and complete these configurations.

a) Use the **Enable Coverage Hole Detection** toggle button to enable or disable Coverage Hole Detection (CHD).

b) Enter data in these fields.

- **Data Packet Count**: enter the minimum threshold for the data packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255.

- **Voice Packet Count**: enter the minimum threshold for the voice packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255.

- **Data Packet Percentage**: enter the threshold for the percentage of the data packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100.

- **Voice Packet Percentage**: enter the threshold for the percentage of the voice packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100.

c) Complete Step 10, on page 859 to Step 13, on page 859 to provision the configuration.

Step 6 Hover your cursor over **6 GHz**, choose **DCA**, and complete these configurations.

a) From the **Channel Assignment Mode** drop-down list, choose a mode.

If you chose **Automatic**, choose the required options from the corresponding drop-down lists.

- **Interval**: choose a DCA interval.
- **Anchortime**: choose an anchor time for DCA.

b) From the **DCA Channel Sensitivity** drop-down list, choose a DCA sensitivity level.

c) From the **Dynamic Bandwidth Selection Max Channel Width** drop-down list, choose the maximum best channel width for DBS.

d) (Optional) Check the **Notification Channel Enable** check box to enable the channel change notification mode.

e) (Optional) Check the **DCA Aggr Startup** check box to enable the aggressive DCA algorithm.

f) In the **DCA Update Interval Sec** field, enter the interval in seconds to specify how often the channel assignment updates are attempted on the AP.

The valid range is from 0 to 4294967295.

g) From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

h) Use the **Include Interference in DCA** toggle button to configure the DCA algorithm to consider detected interference when selecting channels for APs.

This option allows optimization of channel assignments and reduction of co-channel interference.

i) (Optional) In the **Notification Channel Threshold** field, enter the threshold value for triggering channel change notifications.

The valid range is from 1 to 1000.

j) (Optional) Under **Event Driven RRM**, check the **Enable Event Driven RRM** check box to enable event-driven RRM on this band.

If you check this check box, complete these configurations.

- From the **Sensitivity Threshold** drop-down list, choose a threshold level for the event-driven RRM.

  If you chose **Custom**, in the **Custom Threshold** field, enter a custom threshold value for event-driven RRM.

  The valid range is from 1 to 99.

- (Optional) Check the **Rogue contribution** check box to enable event-driven RRM rogue contribution on this band.

  If you check this check box, in the **Rogue Duty-Cycle** field, enter the duty cycle threshold value for event-driven RRM rogue contribution.

  The valid range is from 1 to 99. The default value is 80.

k) Complete Step 10, on page 859 to Step 13, on page 859 to provision the configuration.

Step 7 Hover your cursor over **6 GHz**, choose **TPC**, and complete these configurations.

a) From the **Power Assignment Method** drop-down list, choose a power assignment method.

If you chose **Fixed**, from the **Default Tx Power Level** drop-down list, choose the power level used to transmit data.

b) (Optional) Check the **TPC Channel Aware** check box to indicate that the Transmit Power Control (TPC) algorithm is channel aware.

c) Enter data in these fields.

- **Notification Max Tx Power Threshold**: enter the maximum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

- **Notification Min Tx Power Threshold**: enter the maximum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

d) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Sys Log Tx Power**: enable logging mode for transmission power change
- **Notification Tx Power Enable**: enable transmission power change notification mode

e) Complete Step 10, on page 859 to Step 13, on page 859 to provision the configuration.

Step 8 Hover your cursor over **6 GHz**, choose **RF Grouping**, and complete these configurations.

a) From the **Grouping Mode** drop-down list, choose an RF grouping mode.

b) If you chose the **Leader** grouping mode, under **Static Members**, complete these configurations:

If you want to...	Then...
add a static member	1. Click **Add**. 2. In the **IPv4/IPv6 Address** field, enter a valid IPv4 address or IPv6 address. 3. In the **Controller Name** field, enter the name of the static member. 4. Click **Save**.
delete static members	1. Check the check box for the static member that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

c) (Optional) In the **RRM Group Update Interval (seconds)** field, enter the interval, in seconds, at which RRM group information is updated

Based on this interval, the wireless controller recalculates and applies RRM settings across AP groups. Short intervals provide quick adaption but may increase the system overhead.

d) Complete Step 10, on page 859 to Step 13, on page 859 to provision the configuration.

Step 9 Hover your cursor over **6 GHz**, choose **Spatial Reuse**, and complete these configurations.

a) From the **BSS Color Assignment Mode** drop-down list, choose a BSS color optimization (BCO) mode.

- **Off**: BSS color is not selected dynamically and must be configured manually.
- **Automatic**: BSS color is periodically updated for all APs that permit this operation.

Note For this mode, the DCA channel assignment mode must be automatic in Step 6, on page 857.

b) Complete Step 10, on page 859 to Step 13, on page 859 to provision the configuration.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Configure RRM on the 5-GHz band for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the RRM parameters on the 5-GHz band for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

Step 4 Hover your cursor over **5 GHz**, choose **General**, and complete these configurations.

a) Under **Profile Threshold for Traps**, complete these configurations.

- Enter data in these fields.
  - **Interference Percentage**: enter the interference threshold in percentage.

    The valid range is from 0 to 100. The default value is 10.

    When the interference exceeds this value, traps are generated.
  - **Clients**: enter the threshold number of clients per AP radio to trigger a trap.

    The valid range is from 1 to 200. The default value is 12.
  - **Noise**: enter the noise threshold value.

    The valid range is from -127 to 0. The default value is -70.
  - **Utilization Percentage**, enter the threshold for the bandwidth used by an AP in percentage.

    The valid range is from 0 to 100. The default value is 80.
  - **Throughput (Bps)**: enter the 802.11a throughput threshold.

    The valid range is from 1000 to 10000000. The default value is 1000000.
- (Optional) Check the **Automatic CFG** check box to enable the performance profile mode.

b) Under **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels**, from the drop-down lists, choose the required options.

- **Channel List**: choose a channel option.
- **RRM Neighbor Discover Type**: choose a mode for the NDP.
- **RRM Neighbor Discover Mode**: choose an operating mode for the NDP.

c) Under **Monitor Intervals**, complete these configurations.

- Enter data in these fields.
  - **Neighbor Packet Frequency (sec)**: enter the interval in seconds to specify the frequency of receiving new signal strength, noise, and interference measurements at each AP.

The valid range is from 60 to 3600. The default value is 180.

- **Reporting Interval (sec)**: enter the interval in seconds between each measurement report.

  The valid range is from 60 to 3600. The default value is 180.

- **Neighbor Timeout Factor**: enter the neighbor timeout factor to specify the duration after which the neighbor expires if it doesn't receive its neighbor packets.

  The valid range is from 5 to 60. The default value is 20.

- **Monitor Coverage Interval**: enter the interval in seconds to receive the new coverage measurements at each AP.

  The valid range is from 60 to 3600.

- **Monitor Load Interval**: enter the interval in seconds to receive the new load measurements at each AP.

  The valid range is from 60 to 3600.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Channel Monitor Status**: enable the neighbor monitoring mode.
  - **Monitor RSSI Normalization**: enable 802.11 neighbor discovery RSSI normalization.
  - **Sys Log Load**: enable the logging mode for the load profile.
  - **Sys Log Channel**: enable logging mode for the dynamic channel change.
  - **Sys Log Performance**: enable logging mode for the performance profile.
  - **Sys Log Coverage**: enable logging mode for the coverage profile.
  - **Sys Log Foreign**: enable logging mode for the foreign profile.

- Use the **Log Noise Events** toggle button to log noise-related events detected by the RRM system.

  Logging noise events helps in monitoring and troubleshooting wireless interference issues.

d) Under **UNII-3**, use the **Unii3 Lp Channels** check box to enable or disable UNII-3 low power channels for the 5-GHz band.
e) Complete Step 10, on page 865 to Step 13, on page 865 to provision the configuration.

Step 5 Hover your cursor over **5 GHz**, choose **Coverage**, and complete these configurations.

a) Use the **Enable Coverage Hole Detection** toggle button to enable or disable Coverage Hole Detection (CHD).
b) Enter data in these fields.

- **Data RSSI Threshold**: enter the RSSI threshold for the data packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Voice RSSI Threshold**: enter the RSSI threshold for the voice packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Minimum Failed Client per AP**: enter the minimum number of clients to trigger the CHD algorithm.

The valid range is from 1 to 200. The default value is 3.

- **Percent Coverage Exception Level per AP**: enter the minimum percentage of clients in the coverage hole region of the AP to trigger a coverage hole exception.

  The valid range is from 1 to 100. The default value is 25.

- **Data Packet Count**: enter the minimum threshold for the data packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 50.

- **Voice Packet Count**: enter the minimum threshold for the voice packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 100.

- **Data Packet Percentage**: enter the threshold for the percentage of the data packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

- **Voice Packet Percentage**: enter the threshold for the percentage of the voice packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

c) Complete Step 10, on page 865 to Step 13, on page 865 to provision the configuration.

Step 6 Hover your cursor over **5 GHz**, choose **DCA**, and complete these configurations.

a) Under **Dynamic Channel Assignment Algorithm**, complete these configurations.

- From these drop-down lists, choose the required options.
  - **Channel Assignment Mode**: choose a mode.

    If you chose **Automatic**, from the drop-down lists, choose the required options.
    - **Interval**: choose a DCA interval.
    - **Anchortime**: choose an anchor time for DCA.

  - **DCA Channel Sensitivity**: choose a DCA sensitivity level.
  - **Channel Width**: choose a channel width.
  - **Dynamic Bandwidth Selection Max Channel Width**: choose the maximum best channel width for DBS.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Avoid Foreign AP Interference**: enable the interference detection on the wireless controller
  - **Avoid Persistent Non-Wi-Fi Interference**: enable device detection on the wireless controller.
  - **Avoid Cisco AP load**: enable load detection on the wireless controller.
  - **Zero Wait DFS**: enable the Zero Wait DFS feature.
  - **Avoid Non 5 GHz Noise**: enable the noise detection on the wireless controller.
  - **Notification Channel Enable**: enable the channel change notification mode.

- **DCA Aggr Startup**: enable the aggressive DCA algorithm.

- In the **DCA Min Metric RSSI** field, enter the minimum RSSI energy metric required for DCA to change the channel.

  The valid range is from -100 to -60.

- (Optional) In the **DCA Update Interval Sec** field, enter the interval in seconds to specify how often the channel assignment updates are attempted on the AP.

  The valid range is from 0 to 4294967295.

- From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

b) Use the **Include Interference in DCA** toggle button to configure the DCA algorithm to consider detected interference when selecting channels for APs.

   This option allows optimization of channel assignments and reduction of co-channel interference.

c) (Optional) In the **Notification Channel Threshold** field, enter the threshold value for triggering channel change notifications.

   The valid range is from 1 to 1000.

d) (Optional) Under **Auto-RF Channel List**, check the required check boxes to choose the corresponding RF channels.

e) (Optional) Under **Event Driven RRM**, check the **Enable Event Driven RRM** check box to enable event-driven RRM on the band.

   If you enable event-driven RRM, complete these configurations.

   - From the **Sensitivity Threshold** drop-down list, choose a sensitivity level for the event-driven RRM.

     If you chose the **Custom** sensitivity threshold, in the **Custom Threshold** field, enter the event-driven RRM custom threshold value.

     The valid range is from 1 to 99. The default value is 1.

   - (Optional) Check the **Rogue contribution** check box to enable rogue contribution on the band.

     If you enable rogue contribution, in the **Rogue Duty-Cycle** field, enter the rogue contribution duty cycle threshold.

     The valid range is from 1 to 99. The default value is 80.

f) Complete Step 10, on page 865 to Step 13, on page 865 to provision the configuration.

Step 7 Hover your cursor over **5 GHz**, choose **TPC**, and complete these configurations.

a) From the **Power Assignment Method** drop-down list, choose a power assignment method.

   If you chose **Fixed**, from the **Default Tx Power Level** field, choose a power level used to transmit data.

b) Enter data in these fields.

   - **Maximum Power Level Assignment (dBm)**: enter the upper limit of the transmit power in dBm.

     The valid range is from -10 to 30. The default value is 30.

   - **Minimum Power Level Assignment (dBm)**: enter the lower limit of the transmit power in dBm.

     The valid range is from -10 to 30. The default value is -10.

- **Power Control Threshold (dBm)**: enter the TPC threshold for the RRM algorithm.

  The valid range is from -80 to -50. The default value is -70.

c) (Optional) Check the **TPC Channel Aware** check box to indicate that the TPC algorithm is channel aware.

d) Enter data in these fields.

- **Notification Max Tx Power Threshold**: enter the maximum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

- **Notification Min Tx Power Threshold**: enter the minimum threshold that the TPC algorithm assigns to each radio.

  The valid range is from 3 to 30.

e) (Optional) Check the required check boxes to enable the corresponding configurations.

- **Sys Log Tx Power**: enable logging mode for transmission power change.
- **Notification Tx Power Enable**: enable transmission power change notification mode.

f) Complete Step 10, on page 865 to Step 13, on page 865 to provision the configuration.

Step 8 Hover your cursor over **5 GHz**, choose **RF Grouping**, and complete these configurations.

a) From the **Grouping Mode** drop-down list, choose an RF grouping mode.

b) If you chose the **Leader** grouping mode, under **Static Members**, complete these configurations:

If you want to...	Then...
add a static member	1. Click **Add**. 2. In the **IPv4/IPv6 Address** field, enter a valid IPv4 address or IPv6 address. 3. In the **Controller Name** field, enter the name of the static member. 4. Click **Save**.
delete static members	1. Check the check box for the static member that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

c) (Optional) In the **RRM Group Update Interval (seconds)** field, enter the interval, in seconds, at which RRM group information is updated

Based on this interval, the wireless controller recalculates and applies RRM settings across AP groups. Short intervals provide quick adaption but may increase the system overhead.

d) Complete Step 10, on page 865 to Step 13, on page 865 to provision the configuration.

Step 9 Hover your cursor over **5 GHz**, choose **Spatial Reuse**, and complete these configurations.

a) From the **BSS Color Assignment Mode** drop-down list, choose a BSS color optimization mode.

- **Off**: BSS color is not selected dynamically and must be configured manually.
- **Automatic**: BSS color is periodically updated for all APs that permit this operation.

Note For this mode, the DCA channel assignment mode must be automatic in Step 6, on page 862.

b) Complete Step 10, on page 865 to Step 13, on page 865 to provision the configuration.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Configure RRM on the 2.4-GHz band for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the RRM parameters on the 2.4-GHz band for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

Step 4 Hover your cursor over **2.4 GHz**, choose **General**, and complete these configurations.

a) Under **Profile Threshold for Traps**, complete these configurations.

- Enter data in these fields.
  - **Interference Percentage**: enter the interference threshold in percentage.

    The valid range is from 0 to 100. The default value is 10.

    When the interference exceeds this value, traps are generated.
  - **Clients**: enter the threshold number of clients per AP radio to trigger a trap.

    The valid range is from 1 to 200. The default value is 12.
  - **Noise**: enter the noise threshold value.

    The valid range is from -127 to 0. The default value is -70.
  - **Utilization Percentage**: enter the threshold for the bandwidth used by an AP in percentage.

    The valid range is from 0 to 100. The default value is 80.
  - **Throughput (Bps)**: enter the 802.11a throughput threshold.

    The valid range is from 1000 to 10000000. The default value is 1000000.
- (Optional) Check the **Automatic CFG** check box to enable the performance profile mode.

b) Under **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels**, complete these configurations.

- From the **Channel List** drop-down list, choose a channel option.
- From the **RRM Neighbor Discover Type** drop-down list, choose a mode for the NDP.
- From the **RRM Neighbor Discover Mode** drop-down list, choose an operating mode for the NDP.

c) Under **Monitor Intervals**, complete these configurations.

- Enter data in these fields.
  - **Neighbor Packet Frequency (sec)**: enter the interval in seconds to specify the frequency of receiving new signal strength, noise, and interference measurements at each AP.

    The valid range is from 60 to 3600. The default value is 180.
  - **Reporting Interval (sec)**: enter the interval in seconds between each measurement report.

    The valid range is from 60 to 3600. The default value is 180.

- **Neighbor Timeout Factor**: enter the neighbor timeout factor to specify the duration after which the neighbor expires if it doesn't receive its neighbor packets.

  The valid range is from 5 to 60. The default value is 20.

- **Monitor Coverage Interval**: enter the interval in seconds to receive the new coverage measurements at each AP.

  The valid range is from 60 to 3600.

- **Monitor Load Interval**: enter the interval in seconds to receive the new load measurements at each AP.

  The valid range is from 60 to 3600. The default value is 360.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Channel Monitor Status**: enable the neighbor monitoring mode.
  - **Monitor RSSI Normalization**: enable 802.11 neighbor discovery RSSI normalization.
  - **Sys Log Load**: enable the logging mode for the load profile.
  - **Sys Log Channel**: enable logging mode for the dynamic channel change.
  - **Sys Log Performance**: enable logging mode for the performance profile.
  - **Sys Log Coverage**: enable logging mode for the coverage profile.
  - **Sys Log Foreign**: enable logging mode for the foreign profile.

- Use the **Log Noise Events** toggle button to log noise-related events detected by the RRM system.

  Logging noise events helps in monitoring and troubleshooting wireless interference issues.

d) Complete Step 10, on page 870 to Step 13, on page 871 to provision the configuration.

Step 5 Hover your cursor over **2.4 GHz**, choose **Coverage** and complete these configurations.

a) Use the **Enable Coverage Hole Detection** toggle button to enable or disable Coverage Hole Detection (CHD).

b) Enter data in these fields.

- **Data RSSI Threshold**: enter the RSSI threshold for the data packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Voice RSSI Threshold**: enter the RSSI threshold for the voice packets to trigger the CHD algorithm on the wireless controller.

  The valid range is from -90 to -60. The default value is -80.

- **Minimum Failed Client per AP**: enter the minimum number of clients to trigger the CHD algorithm.

  The valid range is from 1 to 200. The default value is 3.

- **Percent Coverage Exception Level per AP**: enter the minimum percentage of clients in the coverage hole region of the AP to trigger a coverage hole exception.

  The valid range is from 1 to 100. The default value is 25.

- **Data Packet Count**: enter the minimum threshold for the data packet count to trigger the CHD algorithm.

The valid range is from 1 to 255. The default value is 50.

- **Voice Packet Count**: enter the minimum threshold for the voice packet count to trigger the CHD algorithm.

  The valid range is from 1 to 255. The default value is 100.

- **Data Packet Percentage**: enter the threshold for the percentage of the data packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

- **Voice Packet Percentage**: enter the threshold for the percentage of the voice packets dropped to trigger the CHD algorithm.

  The valid range is from 1 to 100. The default value is 50.

c) Complete Step 10, on page 870 to Step 13, on page 871 to provision the configuration.

Step 6 Hover your cursor over **2.4 GHz**, choose **DCA**, and complete these configurations.

a) Under **Dynamic Channel Assignment Algorithm**, complete these configurations.

- From the drop-down lists, choose the required options.
  - **Channel Assignment Mode**: choose a mode.

    If you chose **Automatic**, from the drop-down lists, choose the required options.
    - **Interval**: choose a DCA interval.
    - **Anchortime**: choose an anchor time for DCA.
  - **DCA Channel Sensitivity**: choose a DCA sensitivity level.
  - **Dynamic Bandwidth Selection Max Channel Width**: choose the maximum best channel width for DBS.
- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Avoid Foreign AP Interference**: enable the interference detection on the wireless controller.
  - **Avoid Persistent Non-Wi-Fi Interference**: enable device detection on the wireless controller.
  - **Avoid Cisco AP load**: enable load detection on the wireless controller.
  - **Avoid Non 5 GHz Noise**: enable the noise detection on the wireless controller.
  - **Notification Channel Enable**: enable the channel change notification mode.
  - **DCA Aggr Startup**: enable the aggressive DCA algorithm.
- In the **DCA Min Metric RSSI** field, enter the minimum RSSI energy metric required for DCA to change the channel.

  The valid range is from -100 to -60.
- (Optional) In the **DCA Update Interval Sec** field, enter the interval in seconds to specify how often the channel assignment updates are attempted on the AP.

  The valid range is from 0 to 4294967295.

- From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

b) Use the **Include Interference in DCA** toggle button to configure the DCA algorithm to consider detected interference when selecting channels for APs.

This option allows optimization of channel assignments and reduction of co-channel interference.

c) (Optional) In the **Notification Channel Threshold** field, enter the threshold value for triggering channel change notifications.

The valid range is from 1 to 1000.

d) (Optional) Under **Auto-RF Channel List**, check the required check boxes to choose the corresponding RF channels.

e) Under **Event Driven RRM**, check the **Enable Event Driven RRM** check box to enable event-driven RRM on the band.

If you enable event-driven RRM, complete these configurations.

- From the **Sensitivity Threshold** drop-down list, choose a sensitivity level for the event-driven RRM.

  If you chose the **Custom** sensitivity threshold, in the **Custom Threshold** field, enter the event-driven RRM custom threshold value.

  The valid range is from 1 to 99. The default value is 1.

- (Optional) Check the **Rogue contribution** check box to enable rogue contribution on the band.

  If you enable rogue contribution, in the **Rogue Duty-Cycle** field, enter the rogue contribution duty cycle threshold.

  The valid range is from 1 to 99. The default value is 80.

f) Complete Step 10, on page 870 to Step 13, on page 871 to provision the configuration.

Step 7 Hover your cursor over **2.4 GHz**, choose **TPC**, and complete these configurations.

a) From the **Power Assignment Method** drop-down list, choose a power assignment method.

If you chose **Fixed**, from the **Default Tx Power Level** drop-down list, choose a power level to transmit data.

b) Enter data in these fields.

- **Maximum Power Level Assignment (dBm)**: enter the upper limit of the transmit power in dBm.

  The valid range is from -10 to 30. The default value is 30.

- **Minimum Power Level Assignment (dBm)**: enter the lower limit of the transmit power in dBm.

  The valid range is from -10 to 30. The default value is -10.

- **Power Control Threshold (dBm)**: enter the TPC threshold for the RRM algorithm.

  The valid range is from -80 to -50. The default value is -70.

c) (Optional) Check the **TPC Channel Aware** check box to indicate that the TPC algorithm is channel aware.

d) In the **Notification Max Tx Power Threshold** field, enter the maximum threshold that the TPC algorithm assigns to each radio.

The valid range is from 3 to 30.

e) In the **Notification Min Tx Power Threshold** field, enter the maximum threshold that the TPC algorithm assigns to each radio.

The valid range is from 3 to 30.

f) (Optional) Check the **Sys Log Tx Power** check box to enable logging mode for transmission power change.

g) (Optional) Check the **Notification Tx Power Enable** check box to enable transmission power change notification mode.

h) Complete Step 10, on page 870 to Step 13, on page 871 to provision the configuration.

Step 8 Hover your cursor over **2.4 GHz**, choose **RF Grouping**, and complete these configurations.

a) From the **Grouping Mode** drop-down list, choose an RF grouping mode.

b) If you chose the **Leader** grouping mode, under **Static Members**, complete these configurations:

If you want to...	Then...
add a static member	1. Click **Add**. 2. In the **IPv4/IPv6 Address** field, enter a valid IPv4 address or IPv6 address. 3. In the **Controller Name** field, enter the name of the static member. 4. Click **Save**.
delete static members	1. Check the check box for the static member that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

c) (Optional) In the **RRM Group Update Interval (seconds)** field, enter the interval, in seconds, at which RRM group information is updated

Based on this interval, the wireless controller recalculates and applies RRM settings across AP groups. Short intervals provide quick adaption but may increase the system overhead.

d) Complete Step 10, on page 870 to Step 13, on page 871 to provision the configuration.

Step 9 Hover your cursor over **2.4 GHz**, choose **Spatial Reuse** and complete these configurations.

a) From the **BSS Color Assignment Mode** drop-down list, choose a BSS color optimization mode.

- **Off**: BSS color is not selected dynamically and must be configured manually.
- **Automatic**: BSS color is periodically updated for all APs that permit this operation.

Note For this mode, the DCA channel assignment mode must be automatic in Step 6, on page 868.

b) Complete Step 10, on page 870 to Step 13, on page 871 to provision the configuration.

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Configure RRM FRA parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the RRM FRA parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **RRM**.

Step 4 Click the **FRA** tab.

Step 5 Under **5/6 GHz Flexible Radio Assignment**, complete these configurations.

a) Use the **FRA Status** toggle button to enable or disable Flexible Radio Assignment (FRA) on all APs for 5/6-GHz dual-band (XOR) models.
b) (Optional) Check the **FRA Freeze** check box to enable FRA freeze on all APs for the 5/6-GHz dual-band (XOR) models.
c) From the **FRA Interval** drop-down list, choose an FRA interval for the 5/6-GHz dual-band (XOR) models.

Step 6 Under **2.4/5 GHz Flexible Radio Assignment**, complete these configurations.

a) Use the **FRA Status** toggle button to enable or disable FRA on all APs.
b) (Optional) Check the **FRA Freeze** check box to enable FRA freeze on all APs.
c) From the **FRA Interval** drop-down list, choose an FRA interval.
d) From the **FRA Sensitivity** drop-down list, choose an FRA coverage overlap sensitivity.
e) (Optional) Check the **Client Aware** check box to allow the dual-band to operate in 5-GHz or monitor mode based on the load on the 5-GHz band.
f) From the **FRA Action** drop-down list, choose an FRA action for the dual-band radio.
g) In the **Client Select Threshold** field, enter the FRA utilization threshold value for moving the dual-band radio from the monitor mode to the client-serving mode.

The valid range is from 0 to 100.

Note The client select threshold value must be greater than the client reset threshold value.

h) In the **Client Reset Threshold** field, enter the FRA utilization threshold value for moving the dual-band radio from the client-serving mode to the monitor mode.

The valid range is from 0 to 100.

Note The client reset threshold value must be less than the client select threshold value.

i) From the **FRA Sensor Threshold** drop-down list, choose an FRA sensor threshold value.
j) From the **FRA Service Priority** drop-down list, choose an FRA service priority.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure global wireless parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global wireless parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 In the **Global** tab, enter data in these fields.

- **Secure Network Name Encryption Type**: choose an encryption type to store or transmit the secure network name.

  Note For the clear-text encryption type, the secure network name can contain up to 19 characters. For the AES encryption type, the secure network name must contain 12 to 64 characters.

- **Secure Network Name**: click the edit icon and enter a unique name for the secure network that is used for AP authentication or encryption.

  The name can contain up to 64 characters.

- **Maximum Login Sessions Per User**: enter the maximum number of concurrent logins that are allowed for a single user.

  The valid range is from 0 to 8.

Step 5 Check the required check boxes to enable the corresponding configurations.

- **Wireless Password Policy**: enable wireless password policy for AP join profile (management user password) and flex profile (local auth user password).
- **Management via Wireless**: enable management access from wireless clients
- **AP Lag Mode**: enable the global lag
- **Dot15 Radio**: enable the global 802.15 radio switch
- **Device Classifier**: enable classification of attached devices.

Step 6 Under **Assisted Roaming**, enter data in these fields.

- **Denial Maximum**: enter the maximum number times for association denial.

  The valid range is from 1 to 10.
- **Floor Bias (dBm)**: enter the RSSI bias default value in dBm for APs that are on the same floor.

  The valid range is from 5 to 25.
- **Prediction Minimum**: enter the minimum number of optimized APs for the assisted roaming prediction to work.

  The valid range is from 2 to 6.
- **RSSI Threshold for XOR to Dedicated Mode**: enter the minimum RSSI value in dBm at which an AP switches from dual-band (XOR) mode to dedicated mode.

  The valid range is from -128 to 0. Lower values make the AP mode transition less sensitive to weak signals.

Step 7 (Optional) Under **AP Image Upgrade**, complete these configurations:

- Use the **HTTPS Method** toggle button to enable or disable HTTPS.
- In the **HTTPS Port** field, enter the custom port number for HTTPS file transfer.

  The valid range is from 0 to 65535.

Step 8 (Optional) Under **AP Geolocation**, use the **Geolocation Derivation Using Ranging** toggle button to enable or disable geolocation derivation using ranging to improve AP location accuracy.

Step 9 (Optional) Under **Client Events & Logging**, use these toggle buttons to enable or disable the corresponding configurations:

- **Enable Client Onboarding Event**: enables or disables the generation of events when a new client device joins the wireless network.
- **Enable Detailed Client Syslog**: enables or disables detailed syslog messages for client events.

Step 10 (Optional) Under **Probe Request Management**, complete these configurations:

- **Probe Request Limit**: enter the maximum number of probe requests allowed from a client before taking action.

  The valid range is from 1 to 100.
- **Probe Request Interval (ms)**: enter the minimum interval in milliseconds between probe requests from the same client.

  The valid range is from 100 to 64000.

- **Enable Probe Request Filtering**: enables or disables filtering of probe requests from clients.

  When you enable filtering, wireless controller filters unnecessary probe requests to improve performance and reduce interference.

Step 11 (Optional) Under **Web Authentication**, in the **Web Authentication Max Retries** field, enter the maximum number of times a client can retry web authentication after a failure.

The valid range is from 0 to 20.

Step 12 (Optional) Under **XOR Roaming & Load Balancing**, complete the required configurations:

- **Dedicated to XOR RSSI Threshold (dBm)**: enter the RSSI threshold in dBm for dedicated dual-ban (XOR) operations.

  The valid range is from -128 to 0.

- **Minimum Clients for XOR Roaming**: enter the minimum number of clients required before XOR roaming features are activated.

  The valid range is from 0 to 200.

- **Load Balancing Window**: enter the time in seconds used for load balancing calculations.

  The valid range is from 0 to 200.

- **XOR Roam Probe Suppression Mode**: choose the operational mode for probe suppression during XOR roaming.

- **Probe Suppression Aggressiveness**: enter a number to indicate the aggressiveness level for probe suppression during XOR roaming.

  The valid range is from 0 to 255. A higher value increases suppression to reduce probe traffic.

- **Optimized Roaming Hysteresis**: enter the RSSI in dBm to configure probe cycles to be suppressed.

  The valid range is from -6 to -3.

Step 13 (Optional) Under **Access Point Features**, complete these configurations:

- **LED Brightness Level**: enter a number to indicate the brightness level of AP LEDs.

  The valid range is from 1 to 8. A higher number indicates higher brightness.

- **Use Locally Administered MAC Address**: enables or disables the use of locally administered MAC address for the AP.

  To override the default hardware MAC address for network policies or privacy, enable this option.

Step 14 (Optional) Under **AP Audit & VLAN**, complete these configurations:

- **Enable AP Audit Report**: enables or disables periodic audit reports from APs.

- **AP Audit Report Interval (seconds)**: enter time in seconds to indicate how often APs send audit report to wireless controller.

  The valid range is from 10 to 43200.

- **Persistent VLAN Assignment**: enables or disables persistent VLAN assignment for clients.

  When enabled, clients retain the VLAN assignments across reassociations.

Step 15 Under **AP HTTPS File Transfer**, complete these configurations:

- Use the **File Download** toggle button to enable or disable the HTTPS file download operations for APs.
- Use the **File Upload** toggle button to enable or disable the HTTPS file upload operations for APs.

Step 16 Click **Review and Provision**.

Step 17 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 18 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 19 On the **Tasks** window, monitor the task deployment.

Configure load balancing for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the load-balancing parameters on the 5-GHz and 2.4-GHz bands for a wireless controller and provision the configuration.

For the 6-GHz band, global parameters like **Aggressive Load Balancing Window** and **Aggressive Load Balancing Denial Count** are configured in the RF profile.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **Load Balancing** tab.

Step 5 Under **5 GHz** and **2.4 GHz**, enter data in these fields.

- **Aggressive Load Balancing Window (clients)**: enter the number of clients for the aggressive load-balancing window.

  The valid range is from 0 to 20.

- **Aggressive Load Balancing Denial Count**: enter the denial count for the aggressive load-balancing window.

  The valid range is from 1 to 10.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure band selection for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the band selection parameters per WLAN for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **Band Select** tab.

Step 5 (Optional) Enter data in these fields.

- **Cycle Count**: enter the maximum number of suppression cycles for a client.

  The valid range is from 1 to 10.

- **Cycle Threshold (msec)**: enter a value for the cycle threshold for band selection.

  The valid range is from 1 to 1000.

- **Age Out Suppression (sec)**: enter the expiry time for suppression in seconds.

  The valid range is from 10 to 200.

- **Age Out Dual Band (sec)**: enter the expiry time for dual-band.

  The valid range is from 10 to 300.

- **Client RSSI (dBm)**: enter a minimum value for the mobile station RSSI threshold.

  The valid range is from -90 to -20.

- **Client Mid RSSI (dBm)**: enter the medium mobile station RSSI threshold.

  The valid range is from -90 to -20.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).

Option	Description
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure optimized roaming for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the optimized roaming parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **Optimized Roaming** tab.

Step 5 Under **6 Ghz**, **5 Ghz**, and **2.4 Ghz**, complete these configurations.

a) Use the **Optimized Roaming Mode** toggle button to enable or disable optimized roaming on the corresponding band.
b) From the **Optimized Roaming Data Rate Threshold (mbps)** drop-down list, choose a data rate threshold for 802.11 optimized roaming.

This threshold sets the minimum data rate required for a client to stay connected, encouraging clients to move to better coverage areas.

Note Misconfiguration of data rate threshold may result in client connectivity issues. If you have issues with clients being unintentionally disconnected after enabling this feature, lower or disable the data rate threshold.

c) In the **Optimized Roaming Hysteresis** field, enter the signal strength margin required for client roaming.

The valid range is from 0 to 10.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure high-density parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the high-density parameters on the 5-GHz and 2.4-GHz bands for a wireless controller and provision the configuration.

For the 6-GHz band, the global high-density parameters like **Rx SOP Threshold** and **Multicast Data Rate** are configured in the RF profile.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **High Density** tab.

Step 5 Under **Rx SOP Threshold**, from these drop-down lists, choose the required options.

- **5 GHz (dBm)**: choose a threshold value for the 5-GHz band.

  If you chose **Custom**, in the **Custom 5 GHz (dBm)** field, enter a custom value for the Rx SOP threshold in dBm.

  The valid range is from -85 to -60. The default value is -85.

- **2.4 GHz (dBm)**: choose a threshold value for the 2.4-GHz band.

  If you choose **Custom**, in the **Custom 2.4 GHz (dBm)** field, enter a custom value for the Rx SOP threshold in dBm.

  The valid range is from -85 to -60. The default value is -85.

Step 6 Under **Multicast Data Rate**, from these drop-down lists, choose the required options.

- **5 GHz (dBm)**: choose a minimum data rate at which multicast clients can associate with APs for the 5-GHz band.
- **2.4 GHz (dBm)**: choose a minimum data rate at which multicast clients can associate with APs for the 2.4-GHz band.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Add a preferred call for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to add a preferred call for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **Preferred Calls** tab.

Step 5 Click **Add**.

Step 6 In the **Call Index** field of the **Create Preferred Calls** slide-in pane, enter the SIP index for the call.

The valid range is from 1 to 6.

Step 7 In the **Call Number** field, enter the SIP preferred call number.

The SIP preferred call number can contain up to 28 characters. Catalyst Center does not support ? and spaces in the call number.

Step 8 Click **Review and Provision**.

Step 9 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Configure RFID for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the radio frequency identification (RFID) parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **RFID** tab.

Step 5 Use the **RFID State** toggle button to enable or disable the RFID tag tracking.

Step 6 In the **RFID Timeout (sec)** field, enter the timeout value in seconds to clean up the stale RFID entries.

The valid range is from 60 to 7200.

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).

Option	Description
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure cellular steering for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the cellular steering parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **Cellular Steering** tab.

Step 5 Enter the RSSI threshold value in dBm to trigger the Wi-Fi to cellular steering for the

- 6-GHz band,
- 5-GHz band, and
- 2.4-GHz band.

The valid range is from -90 to -80 dBm.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure 6-GHz client steering for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the 6-GHz client steering parameters per WLAN for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Advanced**.

Step 4 Click the **6 GHz Client Steering** tab.

Step 5 (Optional) Enter data in these fields.

- **6 GHz Transition Minimum Client Count**: enter the minimum number of clients for 6-GHz client steering.

  The valid range is from 0 to 200.

- **6 GHz Transition Minimum Window Size**: enter a value to set the minimum window size of the client steering.

  The valid range is from 0 to 200.

- **6 GHz Transition Max Utilization Difference (%)**: enter a value in percentage to set the maximum channel utilization difference to steer the clients.

  The valid range is from 0 to 100.

- **6 GHz Transition Min 2.4 GHz RSSI Threshold (dBm)**: enter the minimum received 2.4-GHz RSSI threshold to steer the clients.

  The valid range is from -70 to -20.

- **6 GHz Transition Min 5 GHz RSSI Threshold (dBm)**: enter the minimum received 5-GHz RSSI threshold to steer the clients.

  The valid range is from -75 to -20.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure mDNS for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure a multicast Domain Name System (mDNS) gateway for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

Step 4 In the **Global** tab, use the **mDNS Gateway** toggle button to enable or disable the mDNS gateway.

Step 5 If you enable the mDNS gateway, complete these configurations.

- From the **Transport** drop-down list, choose a transport method for mDNS message processing.
- In the **Active-Query Timer (Minutes)** field, enter a time value in minutes.

  The valid range is from 1 to 120. The default value is 30.
- (Optional) From the **mDNS-AP Service Policy** drop-down list, choose an mDNS service policy.

  To create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 890.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an mDNS service definition for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS service definition for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

Step 4 Hover your cursor over **Service Policy** and choose **Service Definition**.

Step 5 Click **Add**.

Step 6 In the **Service Definition Name** field of the **Create Service Definition** slide-in pane, enter a name for the service definition.

The service definition can contain up to 164 characters. It must start with an alphanumeric character.

Step 7 (Optional) In the **Description** field, enter a description.

The description can contain up to 164 characters.

Step 8 Under **Service Types**, configure service types.

If you want to...	Then...
add a service type	**a.** Click **Add**. **b.** In the **Service Type** field of the **Add Service Type** dialog box, enter a string for the service type. You can enter up to 164 characters. Catalyst Center does not allow the special characters ?, <, >, & in the service type. **c.** Click **Save**.
delete service types	**a.** Check the check box next to the service types that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller

You can create mDNS service lists for the ingress and egress directions. Use this procedure to create an mDNS service list for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

Step 4 Hover your cursor over **Service Policy** and choose **Service List**.

Step 5 Hover your cursor over **Add** and choose one of the directions.

- **Direction - IN**: creates service list for the ingress direction.
- **Direction - OUT**: creates service list for the egress direction.

Step 6 In the **Service List Name** field of the **Create Service List** slide-in pane, enter a name for the service list.

The name can contain up to 164 characters.

For the **IN** direction, Catalyst Center does not allow the default-mdns-in-service-list name. For the **OUT** direction, Catalyst Center does not allow the default-mdns-out-service-list name.

Step 7 (Optional) Click the **Assign All Services** toggle button to assign all services to the service list.

If you chose...	Then...
Direction - IN	from the **Message Type** drop-down list, choose a message type.
Direction - OUT	from the **Wired Filter** drop-down list, choose a wired filter. To create a wired filter, see Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 892.

Step 8 (Optional) If the **Assign All Services** toggle button isn't enabled, under **Assigned Services**, configure the services.

If you want to...	Then...
add an available service	**a.** Click **Add**. **b.** From the **Services** drop-down list on the **Add Available Service**, choose a service definition. Catalyst Center automatically populates the string based on the service definition in the **Service String** field. **c.** Based on the chosen direction, complete these configurations. • If you chose **Direction - IN**, from the **Message Type** drop-down list, choose a message type. • If you chose **Direction - OUT**, from the **Wired Filter** drop-down list, choose a wired filter. To create a wired filter, see Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller, on page 892. **d.** Click **Save**.
edit an available service	**a.** Check the check box next to the service that you want to edit. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configuration. **d.** Click **Save**.
delete available services	**a.** Check the check box next to the services that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS service policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

Step 4 Hover your cursor over **Service Policy** and choose **Service Policy**.

Step 5 Click **Add**.

Step 6 In the **Service Policy Name** field of the **Create Service Policy** slide-in pane, enter a unique name for the service policy.

The service policy name can contain up to 164 characters.

Step 7 (Optional) From these drop-down lists, choose the required options.

- **Service List Input**: choose an ingress service list.

  To create an ingress service list, see Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller, on page 889.

- **Service List Output**: choose an egress service list.

  To create an egress service list, see Create an mDNS service list for a Cisco Catalyst 9800 Series Wireless Controller, on page 889.

- **Location**: choose an option for mDNS location-based filtering.
  - **ap-location**: Location-based filtering using the AP location.
  - **ap-name**: Location-based filtering using the AP name.
  - **location-group**: Location-based filtering using the location group.
  - **lss**: Location-based filtering using Location Specific Services (LSS).
  - **regex**: Location-based filtering using a Regular-Expression string.
  - **site-tag**: Location-based filtering using the site tag.
  - **ssid**: Location-based filtering using the SSID.

Step 8 If you chose the **regex** option for location-based filtering using a regular-expression string, complete these configurations.

- From the **AP Regex** drop-down list, choose a corresponding location filtering option.
- In the **Regex Pattern** field, enter the regular-expression string.

  The regex pattern can contain up to 164 characters. Catalyst Center doesn't support ? in this field. If you enter %, +, or * in this field, do not enter any characters after these characters.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create an mDNS wired filter for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS wired filter for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

Step 4 Hover your cursor over **Service Policy** and choose **Wired Filter**.

Step 5 Click **Add**.

Step 6 In the **Wired Filter Name** field of the **Create Wired Filter** slide-in pane, enter a unique name for the wired filter.

The wired filter name can contain up to 64 characters.

Step 7 (Optional) In the **VLAN List** field, enter the list of VLAN IDs.

The valid range for VLAN IDs is from 1 to 4094. You can enter

- multiple VLAN IDs separated by a comma (for example, 20,30,40),
- a range of VLAN IDs (for example, 20-25), or
- up to 16 VLANs in the list separated by a comma (for example, 10-20,30,40-50).

Step 8 Under **MAC Address**, configure the MAC addresses.

If you want to...	Then...
add a MAC address	**a.** Click **Add**. **b.** In the **MAC Address** field of the **Add MAC Address** dialog box, enter the MAC address of an mDNS service provider. Enter the MAC address in the xxxx.xxxx.xxxx format. **c.** Click **Save**.
delete MAC addresses	**a.** Check the check box for the MAC addresses that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create an mDNS flex profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an mDNS flex profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **mDNS**.

Step 4 Click the **mDNS Flex Profile** tab.

Step 5 Click **Add**.

Step 6 In the **mDNS Flex Profile Name** field of the **Create mDNS Flex Profile** slide-in pane, enter a unique name for the mDNS flex profile.

The mDNS flex profile name can contain up to 164 characters. Catalyst Center does not allow ? and spaces in the profile name. The profile name must start with an alphanumeric character.

Step 7 (Optional) Enter data in these fields.

- **Service Cache Update Timer**: enter a value for the mDNS service cache update timer.

  The valid range is from 1 to 100. The default value is 1.

- **Statistics Update Timer**: enter a value for the mDNS statistics update timer.

  The valid range is from 1 to 100.

- **VLAN List**: enter the list of VLAN IDs.

  The valid range for VLAN IDs is from 1 to 4094. You can enter

  - multiple VLAN IDs separated by a comma (for example, 20,30,40),
  - a range of VLAN IDs (for example, 20-25), or
  - up to 16 VLANs in the list separated by a comma (for example, 10-20,30,40-50)

Step 8 (Optional) From the **Wired Service Policy** drop-down list, choose a service policy.

To create a service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 890.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Configure multicast for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the global wireless multicast parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

Step 4 In the **General** tab, use the **Global Wireless Multicast** toggle button to enable or disable global wireless multicast.

If you enable global wireless multicast, you can optionally check the **Wireless mDNS Bridging** check box to enable mDNS bridging.

Step 5 From the **AP CAPWAP Multicast** drop-down, choose a delivery mechanism for the multicast.

If you chose the **Multicast** option, you can optionally enter data in these fields.

- **AP CAPWAP IPv4 Multicast group Address**: enter an IPv4 multicast group address for CAPWAP used by APs.
- **AP CAPWAP IPv6 Multicast group Address**: enter an IPv6 multicast group address for CAPWAP used by APs.

Step 6 Use the toggle buttons to enable or disable these configurations:

- **Wireless Non-IP Multicast**: allows administrators to enable or disable multicast traffic for non-IP applications.
- **Wireless Broadcast**: broadcast traffic transmission within the wireless network.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure IGMP snooping for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure Internet Group Management Protocol (IGMP) snooping for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

Step 4 Click the **IGMP Snooping** tab.

Step 5 (Optional) Check the **IGMP Snooping** check box to enable the IGMP snooping for VLANs.

If you enable IGMP snooping, complete these configurations:

- In the **Last Member Query Interval (msec)** field, enter the last member query interval in milliseconds.

  The valid range is from 100 to 32767.

- (Optional) Under **VLAN(s)**, enable or disable the required VLANs.

  To enable or disable VLANs, check the check box next to the required VLANs, hover your cursor over **Actions** and choose **Enable** or **Disable**.

Step 6 (Optional) Check the **IGMP Snooping Querier** check box to enable the querier when there is no multicast router available in a VLAN to send IGMP membership queries.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure MLD snooping for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure global Multicast Listener Discovery (MLD) snooping for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

Step 4 Click the **MLD Snooping** tab.

Step 5 (Optional) Check the **Snooping** check box to enable global MLD snooping for VLANs.

If you enable MLD snooping, complete these configurations:

- In the **MLD Query Interval (msec)** field, enter the last listener query interval in milliseconds.

  The valid range is either 0 or 100 to 32768.

- (Optional) Under **VLAN(s)**, enable or disable the required VLANs.

  To enable or disable VLANs, check the check box next to the required VLANs, hover your cursor over **Actions** and choose **Enable** or **Disable**.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure PIM and multicast-routing for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure Protocol Independent Multicast (PIM) and multicast routing globally for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

Step 4 Click the **PIM and Multicast-Routing** tab.

Step 5 In the **PIM Configuration** section, configure these parameters:

- **PIM RP-Address**: Enter the Rendezvous Point (RP) address to statically configure the RP Address. This configuration is required so that receivers can find the multicast source in the network.
- **Auto RP Listener**: Enable Auto RP Listener to dynamically discover RP in a PIM-SM network.

Step 6 In the **Multicast Routing Configuration** section, configure these settings:

- **Distributed Multicast-Routing**: Toggle this button to enable or disable the multicast configuration globally.
- **VRF with Distributed Multicast-Routing**: From the list of available VRFs, add or remove the VRFs to be used for distributed multicast-routing. This option enables the segmentation of multicast traffic across multiple virtual networks. To create an VRF interface, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create a VRF to RP address map for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a VRF to Rendezvous Point (RP) address map for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

Step 4 Click the **VRF - RP Address Map** tab.

Step 5 Click **Add**.

Step 6 In the **Create VRF - RP Address Map** slide-in pane, complete these configurations:

- From the **VRF** drop-down list, choose a VRF.

  To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.
- In the **RP Address** field, enter the IP address of the RP for the group.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create wireless broadcast and non-IP multicast for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create VLAN broadcast and non-IP multicast for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Multicast**.

Step 4 Click the **Wireless Broadcast and Wireless Non-IP Multicast** tab.

If the **More** drop-down list is displayed, hover your cursor over **More** and choose **Wireless Broadcast and Wireless Non-IP Multicast**.

Step 5 In the **VLAN ID** field of the **Create VLAN Broadcast and Non-IP Multicast** slide-in pane, enter the VLAN ID.

The valid range is from 1 to 4094.

Step 6 Use these toggle buttons to enable or disable the corresponding configurations:

- **Non-IP Multicast**: enable non-IP muticast for VLANs.
- **Broadcast**: allow broadcast packets for wireless clients.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure location for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the location parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Location**.

Step 4 From the **Algorithm** drop-down list, choose an algorithm used for averaging the RSSI and SNR values.

- **Average**: sets the probe RSSI measurement updates to a more accurate algorithm with more CPU overhead.
- **Simple**: sets the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy.

Step 5 Enter data in these fields.

- **Expiry Calibrating Client Threshold (sec)**: enter the timeout in seconds for calibrating the clients.

  The valid range is from 1 to 3600.

- **Expiry Client Threshold (sec)**: enter the timeout in seconds for RSSI values.

  The valid range is from 5 to 3600.

- **Notify Client Threshold (dB)**: enter the Network Mobility Services Protocol (NMSP) notification RSSI threshold for clients in dB.

  The valid range is from 0 to 10.

  This threshold defines the change in client RSSI that triggers a notification. For example, if you enter 5 in this field, NMSP sends a notification when the RSSI of a client changes by 5 dB.

- **Expiry Tags (sec)**: enter the RFID RSSI expiry time in seconds.

  The valid range is from 5 to 300.

  After the RSSI value expires, the RFID RSSI is cleaned up.

- **Notify Threshold Tags (dB)**: enter the Location Control Protocol (LOCP) notification threshold for RSSI measurements.

The valid range is from 1 to 10.

Step 6 From these drop-down lists, choose the required options.

- **RSSI Half Life Calibrating Client Threshold (sec)**: choose an RSSI half-life threshold for calibrating the clients.
- **RSSI Half Life Client Threshold (sec)**: choose an NMSP notification threshold for the clients.
- **RSSI Half Life Rogue AP Threshold (sec)**: choose an RSSI half-life threshold for rogue APs.
- **RSSI Half Life Tags (sec)**: choose an RSSI half-life threshold for RFID tags.

  RFID RSSI half-life represents the half life when averaging two RSSI readings for RFID tags.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure country codes for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure country codes for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Country**.

Step 4 Configure the country codes.

Use these options to manage country codes:

If you want to...	Then...
search for country codes	in the **Search** field, enter either the partial or full name of the country and press **Enter**.

If you want to...	Then...
add country codes	use one of these options: • Click the plus icon next to the required country code. • Click the country code and click **Add Selected**. **Note** To select and add multiple country codes, press **Shift**, click the country code, and click **Add Selected**.
remove country codes	use one of these options: • Click the **X** icon next to the required country code. • Click the country code and click **Remove Selected**. **Note** To select and remove multiple country codes, press **Shift**, click the country code, and click **Remove Selected**. • Click **Remove All** to remove all the country codes.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Configure Cisco DNA integration settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure Cisco DNA integration settings for a wireless controller and provision the configuration.

Cisco DNA gRPC and Network Assurance gRPC can operate simultaneously. Cisco Spaces IoT Services and Catalyst Center gRPC can also run simultaneously.

Note The clear-text token configuration is available only when **wsaCfgIcapPort** is enabled.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Cisco DNA Integration Settings**.

Step 4 In the **Clear Text Token** field, enter the AP join token in clear-text format.

Use this field when the token type is **Clear** or when you are migrating from unencrypted to encrypted tokens.

Note Clear-text tokens are less secure.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Configure AP policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the AP policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.
a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.
a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **AP Policy**.

Step 4 Click the **AP Policy** tab.

Step 5 (Optional) Check the required check boxes to configure the corresponding policies.

- **Authorize APs against MAC**: configure the AP authorization policy with the MAC address
- **Authorize APs against Serial Number**: configure the AP authorization policy with the serial number

Step 6 From the **Authorization Method List** drop-down list, choose an authorization method list.

To create an authorization method list for **Type - Credential-download**, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create a device authentication serial number for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a device authentication serial number for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **AP Policy**.

Step 4 Hover your cursor over **Device Authentication** and choose **Serial Numbers**.

Step 5 Click **Add**.

Step 6 In the **Serial Number** field of the **Create Device Authentication Serial Number** slide-in pane, enter the device authentication serial number.

It can contain up to 255 characters. Catalyst Center does not support ? and spaces in the serial number.

Step 7 (Optional) From the **Attribute List Name** drop-down list, choose an attribute list.

To create an attribute list, see Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller, on page 783.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a device authentication MAC Address for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a device authentication MAC address for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **AP Policy**.

Step 4 Hover your cursor over **Device Authentication** and choose **MAC Addresses**.

Step 5 Click **Add**.

Step 6 In the **MAC Address** field of the **Create Device Authentication MAC Address** slide-in pane, enter the device authentication MAC address.

It can contain up to 64 characters. You can enter the MAC address in the *xx:xx:xx:xx:xx:xx*, *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, or *xxxxxxxxxxxx* format.

Step 7 (Optional) From the **Attribute List Name** drop-down list, choose an attribute list.

To create an attribute list, see Create an attribute list for a Cisco Catalyst 9800 Series Wireless Controller, on page 783.

Step 8 (Optional) In the **Description** field, enter a description.

You can enter up to 128 characters. Catalyst Center does not support ? in the description.

Step 9 (Optional) From the **WLAN Profile Name** drop-down list, choose a WLAN profile.

To create a WLAN profile, see Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 683.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Configure wireless geolocation settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure wireless geolocation settings for APs associated with a wireless controller to enable location-based services and tracking capabilities, and then provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Global Wireless** and click **Wireless Geolocation Settings**.

Step 4 Use the **Enable Geolocation Derivation** toggle button to enable or disable the automatic update and derivation of geographic location of APs.

When you enable this option, the wireless controller automatically derives and updates the geographic location of APs using available network data. This option improves location-based services and reporting. If you disable this option, you must manually configure geolocation settings for each AP.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Service configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device service configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create a service template for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a service template for a local policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Local Policy**.

Step 4 In the **Service Template** tab, click **Add**.

Step 5 Enter data in these fields of the **Create Service Template** slide-in pane.

- **Service Template Name**: enter a unique name for the service template.

  The name can contain up to 48 characters.

- (Optional) **VLAN ID**: enter a VLAN ID.

  The valid range is from 1 to 4094.

- (Optional) **Session Timeout (sec)**: enter the session timeout in seconds.

  The valid range is from 1 to 1073741823.

Step 6 (Optional) From these drop-down lists, choose the required options.

- **Access Control List** (to create an ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785)
- **Ingress QoS** (to create a QoS, see Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 910)
- **Egress QoS** (to create a QoS, see Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 910)
- **mDNS Service Policy** (to create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 890)

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create a policy map for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a policy map and map it to a service template for a local policy for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Local Policy**.

Step 4 Click the **Policy Map** tab.

Step 5 Click **Add**.

Step 6 In the **Policy Map Name** field of the **Create Policy Map** slide-in pane, enter a unique name for the policy map.

Step 7 (Optional) Under **Match Criteria List**, configure the required match criteria list.



Note Configure at least one match criteria list. You can configure up to 254 match criteria lists.

If you want to...	Then...
add a match criteria list	**a.** Click **Add**. **b.** From the **Service Template** drop-down list of the **Add Match Criteria List** dialog box, choose a service template for the local policy. To create a service template, see Create a service template for a Cisco Catalyst 9800 Series Wireless Controller, on page 907. **c.** (Optional) Check the required check boxes to include the corresponding filters in the match criteria list. • **Device Type** • **User Role** • **User Name** • **OUI** • **MAC Address** **d.** If you checked the check box for any filter, complete these configurations. • From the corresponding **Condition** drop-down list, choose a condition for the filter: **equals**, **does not equal**, or **regex** • Enter data in the corresponding field for the filter: • **Device Type**: enter the device name. • **User Role**: enter the user role. • **User Name**: enter the user name. • **OUI**: enter an Organizationally Unique Identifier (OUI) in hexadecimal format separated by a period. For example, *xx.xx.xx*. • **MAC Address**: enter a MAC address in the *xxxx.xxxx.xxxx* format. **e.** Click **Save**.
edit a match criteria list	**a.** Check the check box next to the sequence that you want to edit. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.

If you want to...	Then...
delete match criteria lists	**a.** Check the check box next to the sequences that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a QoS policy for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a QoS policy for a wireless controller and provision it.

Note You must add at least one class map or configure class default for a QoS policy.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **QoS**.

Step 4 Click **Add**.

Step 5 In the **Policy Name** field of the **Create QoS Policy** slide-in pane, enter a unique name for the QoS policy.

Catalyst Center does not allow ? and spaces in the policy name.

Step 6 (Optional) In the **Description** field, enter a description.

The description can contain up to 200 characters.

Step 7 Under **Class Default**, complete these configurations.

a) From the **Mark Type** drop-down list, choose the required option: **None**, **DSCP**, or **User Priority**.

Marking can be used to either

- set certain fields or bits in the packet headers, or
- set certain fields in the packet structure that is internal to the device.

If you chose...	Then...
DSCP	from the **Mark Value** drop-down list, choose the required option to set DSCP in IPv4 and IPv6 packets.
User Priority	from the **Mark Value** drop-down list, choose the required option to set the WLAN user priority.

b) (Optional) In the **Police (kbps)** field, enter the committed information rate.

The valid range is from 8 to 10000000.

Step 8 (Optional) Under **Class Maps**, configure class maps.

a) Click **Add** to add a class map.

In the **Add Class Map** dialog box, complete these configurations.

1. From the **Class Type** drop-down list, choose a class map type: **AVC** or **User Defined**.
2. From the **Match** drop-down list, choose a match type: **Any** or **All**.
3. From the **Drop** drop-down list, choose the required option to drop traffic from specific sources: **Disabled** or **Enabled**.

   If you chose **Disabled**, complete these configurations.

   - From the **Mark Type** drop-down list, choose the required option: **None**, **DSCP**, or **User Priority**.

If you chose...	Then...
DSCP	from the **Mark Value** drop-down list, choose the required option to set DSCP in IPv4 and IPv6 packets.
User Priority	from the **Mark Value** drop-down list, choose the required option to set the WLAN user priority.

   - (Optional) In the **Police (kbps)** field, enter the committed information rate.

     The valid range is from 8 to 10000000.

4. From the **Match Type** drop-down list, choose the required matching parameter.

If you chose...	Then...
the **AVC** class type	add a matching parameter based on the match type using one of these methods: • Click the plus icon next to the required matching parameter. • Click the required matching parameter and click **Add Selected**. To choose multiple matching parameters, press **Shift**, click the matching parameter, and click **Add Selected**. • To add all the matching parameters, click **Add All**. You can use the **Search** field to filter the matching parameter. Add at least one matching parameter. You can add up to 256 matching parameters. For example, if you chose the **Protocol** match type, choose at least one protocol.
the **User Defined** class type	from the **Match Value** drop-down list, choose the required matching parameter.

5. Click **Save**.

b) To delete a class map, complete these steps.

1. Check the check box next to the required class map.
2. Hover your cursor over **Actions** and choose **Delete**.
3. In the dialog box, click **Yes**.

Step 9 Click **Review and Provision**.

Step 10 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create a custom application for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a custom application for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Application Visibility**.

Step 4 In the **Custom Applications** tab, click **Add**.

Step 5 In the **Application Name** field of the **Create Custom Application** slide-in pane, enter a unique name for the application.

The application name length must be between 3 and 24 characters. Catalyst Center allows alphanumeric characters, - and _ in the application name. Catalyst Center does not allow spaces and other special characters in the application name.

Step 6 From the **Type** drop-down list, choose an application type: **URL**, **Server Name**, **Protocol**, or **DSCP**.

Step 7 Based on the application type, complete these configurations.

a) If you choose **URL**, in the **URL** field, enter the URL.

Catalyst Center does not allow spaces in the URL.

b) If you choose **Server Name**, in the **Server Name** field, enter the server name.

You can enter up to 30 characters.

c) If you choose **Protocol**, complete these configurations:

- In the **IP Address** field, enter a valid IP address of the custom application in the *x.x.x.x* format.
- (Optional) In the **Subnet (0-32)** field, enter the subnet mask of the custom application.

  The valid range is from 0 to 32.
- Under **Protocol Type**, check the check box next to the required protocols: **TCP** and **UDP**
- Under **Port Values**, choose the required option.

- If you choose **Individual Values**, complete these configurations:

If you want to...	Then...
add a port number	1. Click **Add**. 2. In the **Port Number** field of the **Add Port Number** dialog box, enter a port number. The valid range is from 1 to 65535. 3. Click **Save**.
delete port numbers	1. Check the check box next to the port numbers that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

- If you choose **Range**, enter the start and end range for the port number in the corresponding fields.

  The valid range is from 1 to 65535.

d) If you choose **DSCP**, use one of these methods to add DSCP.

Note Add at least one DSCP.

- Click the plus icon next to the required DSCP.
- Click the required DSCP and click **Add Selected**.

  To choose multiple DSCP, press **Shift**, click the DSCP, and click **Add Selected**.
- To add all the DSCP, click **Add All**.

  You can use the **Search** field to filter the DSCP.

Step 8 Choose either **Traffic Class** or **Similar To**.

If you chose...	Then...
Traffic Class	from the **Traffic Class** drop-down list, choose a class.
Similar To	from the **Similar To** drop-down list, choose the required option.

Step 9 From the **Business Relevance** drop-down list, choose an option: **Relevant**, **Irrelevant**, or **Default**.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create an exporter for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a flow exporter for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Application Visibility**.

Step 4 Hover your cursor over **Flow Monitors** and click **Exporter**.

Step 5 In the **Exporter** window, click **Add**.

Step 6 In the **Create Exporter** slide-in pane, complete these configurations:

a) In the **Exporter Name** field, enter a unique name for the flow exporter.

You can enter up to 60 characters. Catalyst Center allows alphanumeric characters, - and _ in the exporter name. Catalyst Center does not allow spaces and other special characters in the exporter name.

b) (Optional) In the **Description** field, enter a description for the flow exporter.

You can enter up to 80 characters. Catalyst Center does not allow the special characters ?, <, >, and & in the exporter name.

c) From the **Exporter Type** drop-down list, select an exporter type: **External Collector** or **Local**.

If you select **External Collector**, complete these configurations:

- **Destination IP**: Enter the IP address of the destination and the flow records are sent to this destination device. Enter the IP address in the *xxx.xxx.xxx.xxx* format.
- **VRF**: Select a VRF from the drop-down list. The flow monitor is associated with the selected VRF.
- **Port**: Enter the UDP port number.

  The valid range is from 1 to 65535. The default value is 9995.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create a flow monitor for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a flow monitor for a wireless controller and provision it.

Before you begin

Ensure that you have created flow exporters to be bound to the flow monitor.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Application Visibility**.

Step 4 Hover your cursor over **Flow Monitors** and click **Monitor**.

Step 5 In the **Monitor** window, click **Add**.

Step 6 In the **Create Monitor** slide-in pane, enter the configuration settings:

- **Flow Monitor Name**: Enter a unique name for the flow monitor.

  You can enter up to 40 characters. Catalyst Center allows the special characters -, _, @, [,], {, }, (,), and . in the flow monitor name.

- (Optional) **Description**: Enter a description for the flow monitor.

  You can enter up to 80 characters. Catalyst Center does not allow ? in the flow monitor name.

- **Flow Exporters**: Use one of these methods to add the required flow exporters from the available list.
  - Click the plus icon next to the required flow exporter.
  - Click the required flow exporter and click **Add Selected**.

    To choose multiple flow exporter, press **Shift**, click the flow exporter, and click **Add Selected**.

- To add all the flow exporter, click **Add All**.

  You can use the **Search** field to filter the flow exporter.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure EoGRE global parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the EoGRE global parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **EoGRE**.

Step 4 In the **Global** tab, enter data in these fields.

- **Heartbeat Interval(sec)**: enter the heartbeat interval in seconds for keepalive to the tunnel gateway.

  The valid range is from 60 to 600.

- **Max Heartbeat Skip Count**: enter the maximum heartbeat skip count for keepalive to the tunnel gateway.

  The valid range is from 3 to 10.

Step 5 From the **Interface Name** drop-down list, choose an interface.

To manage physical interfaces, Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller, on page 939

To create an SVI profile, see Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 930.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an EoGRE gateway for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EoGRE tunnel gateway for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **EoGRE**.

Step 4 Click the **Gateways** tab.

Step 5 Click **Add**.

Step 6 In the **Tunnel ID** field of the **Create Gateway** slide-in pane, enter the tunnel ID.

Step 7 Under **Destination IP Address**, choose an IP address option.

Step 8 (Optional) From the **Source Interface** drop-down list, choose an interface.

To manage physical interfaces, see Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller, on page 939.

To create an SVI profile, see Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 930.

Step 9 (Optional) Based on the destination IP address option that you chose, complete these configurations.

If you chose...	Then...
Ipv4	in the **Destination IP Address(IPv4)** field, enter the destination IPv4 address or host name.
Ipv6	in the **Destination IP Address(IPv6)** field, enter the destination IPv6 address or host name.

Step 10 (Optional) Click the **AAA Proxy** toggle button to enable AAA proxy and complete these configurations.

- From the **Encryption Type** drop-down list, choose an encryption type.
- Enter data in these fields.
  - **Key Phrase**: enter the AAA key phrase.

    You can enter up to 128 characters.
  - **Auth Port**: enter the AAA authentication or authorization port.

    The valid range is from 0 to 65535.
  - **Acct Port**: enter the AAA accounting port.

    The valid range is from 0 to 65535.

Step 11 Click **Review and Provision**.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create an EoGRE domain for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EoGRE tunnel domain for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **EoGRE**.

Step 4 Click the **Domains** tab.

Step 5 Click **Add**.

Step 6 In the **Domain Name** field of the **Create Domain** slide-in pane, enter a name for the tunnel domain.

Step 7 (Optional) Click the **Status** toggle button to enable the tunnel domain.

Step 8 (Optional) Choose a primary and secondary tunnel gateway from the corresponding drop-down lists.

Step 9 (Optional) Check the **Revertive Redundancy** check box to enable the revertive redundancy model.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create an EoGRE tunnel profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an EoGRE wireless tunnel profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **EoGRE**.

Step 4 Click the **Tunnel Profiles** tab.

Step 5 Click **Add**.

Step 6 In the **General** tab of the **Create Tunnel Profile** slide-in pane, complete these configurations.

a) In the **Tunnel Profile Name** field, enter a name for the tunnel profile.

The tunnel profile name can contain up to 128 characters.

b) (Optional) Click the **Status** toggle button to enable the tunnel profile.
c) Use the **Centralized Forwarding** toggle button to indicate whether all wireless client traffic is routed through the central controller or forwarded locally to the AP.
d) Under **DHCP Option-82**, complete these configurations.

- (Optional) Click the **DHCP Option-82 Status** toggle button to enable the DHCP Option 82.
- (Optional) Click the **ASCII** toggle button to enable the DHCP Option 82 in ASCII format.

  If the ASCII format isn't used, the binary format is used.
- (Optional) In the **Delimiter** field, enter the DHCP Option 82 delimiter character.

You can enter a single delimiter character.

- From these drop-down lists, choose the required options.
  - **MAC Format**: choose a DHCP Option 82 MAC format.
  - (Optional) **Circuit ID**: choose a DHCP Option 82 circuit ID.
  - (Optional) **Remote ID**: choose a DHCP Option 82 remote ID.

e) (Optional) Under **AAA**, check the required check boxes to enable the corresponding configurations.

- **RADIUS Proxy**: enable AAA proxy.

  If you enable AAA proxy, you can optionally check the **Accounting Proxy** check box to enable AAA accounting proxy.
- **Override**: enable AAA override.

Step 7 (Optional) Click the **Rules** tab and configure the required rules.

If you want to...	Then...
add a rule	**a.** Click **Add**. **b.** In the **Priority** field of the **Add Rule** dialog box, enter a number for the rule priority. The valid range is from 1 to 100. **c.** In the **Realm** field, enter the rule realm to match with. The rule realm can contain up to 128 characters. Catalyst Center does not support leading or trailing spaces in the realm. **d.** From the **Domain Name** drop-down list, choose a destination domain for the rule. **e.** In the **VLAN ID** field, enter the rule VLAN ID. The valid range is from 1 to 4094. **f.** Click **Save**.
edit a rule	**a.** Check the check box next to the rule that you want to edit. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete rules	**a.** Check the check box next to the rules that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure media stream for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the media stream parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Media Stream**.

Step 4 In the **General** tab, use the **Enable Multicast Direct** toggle button to enable or disable the multicast-direct configuration.

Step 5 (Optional) Under **Session Message Configuration**, complete these configurations.

a) Check the **Session Announcement State** check box to enable the media stream Session Description Protocol (SDP) message.
b) Enter data in these fields.

- **Session Announcement URL**: enter the media stream SDP URL.

  The URL can contain up to 128 characters.

- **Session Announcement Email**: enter the media stream SDP email ID.

  The email ID can contain up to 64 characters.

- **Session Announcement Phone**: enter the media stream SDP phone number.

  The phone number can contain up to 30 numbers and hyphens.

- **Session Announcement Note**: enter the media stream SDP announcement note.

  The announcement note can contain up to 128 characters.

Step 6 Click **Review and Provision**.

Step 7 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create a media stream profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a media stream profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Media Stream**.

Step 4 Click the **Streams** tab.

Step 5 Click **Add**.

Step 6 In the **Media Stream Name** field of the **Create Media Stream Profile** slide-in pane, enter a name for the media stream group.

The media stream group name can contain up to 64 characters.

Step 7 In the **Maximum Expected Bandwidth (Kbps)**, enter the expected bandwidth for the media stream.

The valid range is from 1 to 35000. The default value is 1000.

Step 8 Under **Multicast Destination**, enter valid IPv4 address or IPv6 address in these fields.

- **Start IPv4/IPv6 Address**: enter the media stream group starting IP address.
- **End IPv4/IPv6 Address**: enter the media stream group ending IP address.

  The starting and ending IP addresses must be of the same type.

Step 9 Under **Resource Reservation Control (RRC) Parameters**, from the drop-down lists, complete these configurations.

a) In the **Average Packet Size (bytes)** field, enter the expected packet size for the stream.

The valid range is from 100 to 1500. The default value is 1200.

b) From these drop-down lists, choose the required options.

- **Policy**: choose an action for the stream: **Admit** or **Deny**
- **Priority**: choose a priority for the stream. You can choose a value from 1 to 8.
- **QoS**: choose a QoS value for the stream.
- **RRC re-evaluation**: choose an option for the RRC evaluation: **Periodical** or **Initial**
- **Violation**: choose an action for RRC violation: **Fallback** or **Drop**

Step 10 Click **Review and Provision**.

Step 11 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create a guest LAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a guest LAN profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Guest LAN**.

Step 4 In the **Guest LAN Profiles** tab, click **Add**.

Step 5 In the **General** tab of the **Create Guest LAN Profile** slide-in pane, complete these configurations.

a) In the **Guest LAN Profile Name** field, enter a unique name for the guest LAN profile.

The profile name can contain up to 32 characters.

b) In the **ID** field, enter an ID for the guest LAN profile.

The valid range is from 1 to 5.

c) In the **Client Association Limit** field, enter the maximum number of client connections per a guest LAN.

The valid range is from 1 to 2000. The default value is 2000.

d) From the **mDNS Mode** drop-down list, choose an mDNS mode for the guest LAN: **Bridging**, **Drop**, or **Gateway**
e) Use the **Wired VLAN Status** toggle button to enable or disable a wired-VLAN ID for the guest LAN.

Note The wired-VLAN ID must be configured on the guest foreign controller.

If you enable the wired-VLAN ID, in the **Wired VLAN ID** field, enter the VLAN ID for the guest LAN on the guest foreign controller.

The valid range is from 0 to 4094. The default value is 0.

f) Use the **Status** toggle button to enable or disable the guest LAN.

Step 6 (Optional) Click the **Security** tab and complete these configurations.

a) Check the **Web Auth** check box to configure security web authentication.

b) From these drop-down lists, choose the required options.

- **Web Auth Parameter Map** (to create a web authentication profile, see Create a web authentication profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 809)
- **Authentication List** (to create an authentication list, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776)
- **Authorization List** (to create an authorization list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777)

Step 7 Click **Review and Provision**.

Step 8 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a guest LAN map for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a guest LAN map for a wireless controller and provision it.

Note You can create a single guest LAN map for a wireless controller.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Guest LAN**.

Step 4 Click the **Guest LAN Map** tab.

Step 5 Click **Add**.

Step 6 In the **Map Name** field of the **Create Guest LAN Map** slide-in pane, enter a unique name for the guest LAN map.

The map name can contain up to 32 characters.

Step 7 (Optional) Under **Guest LAN - Policy Map**, configure guest LAN and policy map profile.

Note You can configure up to five guest LAN and policy profile maps.

If you want to...	Then...
add a guest LAN and policy profile map	**a.** Click **Add**. **b.** From the **Guest LAN Profile Name** drop-down list on the **Add Guest LAN - Policy Map** dialog box, choose a guest LAN profile. **c.** From the **Policy Profile Name** drop-down list, choose a policy profile. **d.** Click **Save**.
edit a guest LAN and policy profile map	**a.** Check the check box next to the required profile name. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the required configurations. **d.** Click **Save**.
delete guest LAN and policy profile maps	**a.** Check the check box next to the required profile names. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 If the wireless controller manages APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, choose the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue to device provision	Continue with the device provisioning. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Add an excluded client for a Cisco Catalyst 9800 Series Wireless Controller

Excluded clients can be used for troubleshooting or security purposes. By excluding the required clients, you can ensure that certain devices aren't able to access the network.

Use this procedure to add an excluded client for a wireless controller and provision it.

Note If you modify the list of clients from the Assurance window, the **Excluded Clients** table displays them only after the wireless controller is resynchronized.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **Excluded Clients**.

Step 4 Click **Add**.

Step 5 In the **Create Client Exclusion** slide-in pane, enter data in these fields.

- **Client device MAC Address**: enter the MAC address of the client that you want to exclude.

  Enter the MAC address in *xxxx.xxxx.xxxx*, *xx-xx-xx-xx-xx-xx*, *xxxx-xxxx-xxxx*, *xxxx:xxxx:xxxx*, or *xx:xx:xx:xx:xx:xx* format. Ensure that the client is not already on the exclusion list.

- **Description**: enter a description for the MAC address or a reason for exclusion.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure ThousandEyes for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to enable ThousandEyes wireless active testing and provision the configuration on a wireless controller.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Services** and click **ThousandEyes**.

Step 4 In the **ThousandEyes Configuration** window, complete these configurations:

a) Use the **Wireless Active Testing Status** toggle button to enable or disable wireless active testing on the wireless controller.

When enabled, compatible APs can act as synthetic wireless clients to run ThousandEyes tests. ThousandEyes provides visibility from the AP to the cloud for proactive network assurance.

b) (Optional) In the **TE Connection String** field, enter the unique token that identifies the ThousandEyes account group for Endpoint Agent registration.

Obtain the token from the ThousandEyes Enterprise Agent application under **Endpoint Experience** > **Agent Settings** by clicking **Download** or **Add New Endpoint Agent**.

c) (Optional) Review the **TE Download URL** field and update it only if necessary.

By default, this field contains the URL for downloading and installing the ThousandEyes Endpoint Agent package on compatible APs.

What to do next

Active testing APs require specific tag configurations to operate as synthetic wireless clients. Review and configure the required profiles and tags for your active testing APs:

- Configure a dedicated RF tag using a radio profile with the **Wireless Active Testing Radio Selection** enabled. This configuration allows the active testing AP radio to operate in synthetic client mode. Refer to Create a radio profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 720 and Create an RF tag for a Cisco Catalyst 9800 Series Wireless Controller, on page 722.
- Use an existing policy tag for the active testing AP. The active testing AP does not broadcast SSIDs from the policy tag. The SSID names in the policy tag are sent to ThousandEyes to support test configuration. Refer to Create a WLAN profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 683, Create a policy profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 696, and Create a policy tag for a Cisco Catalyst 9800 Series Wireless Controller, on page 710.
- Use a site tag with an AP join profile that has Application Hosting enabled. This setting allows the ThousandEyes Endpoint Agent container to run on the AP. Refer to Create a site tag for a Cisco Catalyst 9800 Series Wireless Controller, on page 758 and Create an AP join profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 728.
- Assign the RF tag, policy tag, and site tag to the active testing AP through tag mapping. This step ties the required configurations together and places the AP into active testing operation. Refer to Tag mapping configurations for a Cisco Catalyst 9800 Series Wireless Controller, on page 761.
- Validate the operational state from the ThousandEyes Enterprise Agent application dashboard and the Catalyst Center Assurance or telemetry workflow.

Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device Layer 2 configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Switched VLAN Interface (SVI) profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **VLAN**.

Step 4 In the **SVI** tab, click **Add**.

Step 5 In the **General** tab of the **Create SVI** slide-in pane, complete these configurations.

a) In the **VLAN Number** field, enter a VLAN ID for SVI.

The valid range is from 1 to 4094.

b) (Optional) In the **Description** field, enter a description.
c) Use the **Admin Status** toggle button to enable or disable the VLAN.
d) (Optional) From the **VRF** drop-down list, choose a VRF.



Important VRF modification results in the removal of IPv4 and IPv6 addresses.

e) (Optional) In the **MTU (bytes)** field, enter the value for IP MTU.

The valid range is from 68 to 18000. The default value is 1500.

f) (Optional) Check the **PIM Sparse Mode** check box to enable Protocol Independent Multicast (PIM) sparse mode for efficient multicast routing.

We recommend this mode for networks with sparse receiver distribution.

g) (Optional) From the **IGMP Version** drop-down list, choose an IGMP version.
h) (Optional) Check the **Autostate** check box to enable automatic state determination for VLAN.
i) (Optional) Check the **IPv4** check box to enable IPv4 addresses on the VLAN interfaces and complete these configurations.

- From the **Type** drop-down list, choose the method through which VLAN interfaces receive their IP configuration.
- If you choose **Static**,
  - In the **IP Address** field, enter an IPv4 address.
  - In the **Subnet Mask** field, enter a subnet mask.
  - Check the **Secondary** check box to add a secondary IP address.

    If you check this check box, enter the secondary IP address and subnet mask in the corresponding fields.
- If you choose **DHCP**, in the **Host Name** field, enter the host name.

- Under **OSPF**, complete these configurations.
  - From the **Process ID** drop-down list, choose an Open Shortest Path First (OSPF) process ID.
  - Check the **BFD** check box to enable Bidirectional Forwarding Detection (BFD).
  - Check the **Message Digest Authentication** check box to use message-digest authentication.
  - Under **Message Digest Authentication - Key Map(s)**, configure message digest authentication key map.

If you want to...	Then...
add a message digest authentication key map	1. Click **Add**. 2. In the **Key** field, enter the key. 3. In the **Password Type** field, enter the encryption type. 4. In the **Password** field, enter the OSPF key. 5. Click **Save**.
delete message digest authentication key map	1. Check the check box next to the keys that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

j) (Optional) Check the **IPv6** check box to enable IPv6 addresses on the VLAN interfaces and complete these configurations.

- Configure IPv6 static.

If you want to...	Then...
add an IPv6 static	1. Click **Add**. 2. From the **Type** drop-down list in the **Add IPv6 Static** dialog box, choose a type. 3. In the **Address** field, enter the address for the VLAN interface. 4. Click **Save**.
delete IPv6 static	1. Check the check box next to the IPv6 addresses that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

- (Optional) Check the required check boxes to enable the corresponding configurations.
  - **Link Local**: use link-local address.

    If you check this check box, in the **Address** field, enter the link-local address.

- **DHCP**: enable DHCP to allow SVI to dynamically obtain an IPv6 address.

  If you enable DHCP, you can optionally check the **Rapid Commit** check box to enable rapid commit for prefix delegation.

- **Autoconfig**: enable automatic address assignment on VLAN interfaces.

  If you check this check box, you can optionally check the **Default** check box to insert the default route.

- **Act as an IPv6 DHCP client**: enable automatic IPv6 address assignment from DHCP servers.

  If you check this check box, in the **Prefix Name** field, you can optionally enter the prefix name.

  You can enter up to 200 characters for the prefix name.

Step 6 (Optional) Click the **Advanced** tab and complete these configurations.

a) Under **Access Lists**, choose an inbound and outbound IPv4 and IPv6 ACL from the corresponding drop-down lists.

To create an ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785 and Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792.

b) Under **DHCP Relay**, complete these configurations.

- Check the **Relay Information Option** check box to enable the relay information option in the received DHCP.
- In the **Subscriber ID** field, enter the subscriber ID suboption.
- From the **Source-Interface VLAN** drop-down list, choose an SVI.

  To create an SVI profile, see Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 930.

- Check the **Server Id Override** check box to insert server-id-override and link-selection suboption.
- Check the **Option Insert** check box to allow insertion of DHCP options in outbound packets.

c) Under **Helper Address(es)**, configure the IPv4 helper addresses.

If you want to...	Then...
add a helper address	1. Click **Add**. 2. In the **IPv4 Helper Address** field of the **Add Helper Address** dialog box, enter the DHCP server IP address. 3. Click **Save**.
delete a helper address	1. Check the check box next to the helper addresses that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

d) Check the **mDNS Gateway** check box to enable mDNS gateway.

Ensure that the mDNS gateway is configured in the global configuration mode. For more information, see Configure mDNS for a Cisco Catalyst 9800 Series Wireless Controller, on page 886.

(Optional) If you check this check box, from the **mDNS Service Policy** drop-down list, choose an mDNS service policy. To create an mDNS service policy, see Create an mDNS service policy for a Cisco Catalyst 9800 Series Wireless Controller, on page 890.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create a VLAN profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a VLAN profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **VLAN**.

Step 4 Click the **VLAN** tab.

Step 5 Click **Add**.

Step 6 In the **VLAN ID** field of the **Create VLAN** slide-in pane, enter a VLAN ID.

The valid range is from 1 to 4094.

Step 7 In the **Vlan Name** field, enter a VLAN name.

Step 8 From the **State** drop-down list, choose an operational state for the VLAN.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Create a VLAN group profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a VLAN group profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **VLAN**.

Step 4 Click the **VLAN Group** tab.

Step 5 Click **Add**.

Step 6 In the **VLAN Group Name** field of the **Create VLAN Group** slide-in pane, enter a VLAN group name.

Step 7 In the **VLAN List** field, enter a value for the VLAN list.

You can enter either

- a VLAN ID (the valid range for VLAN ID is from 1 to 4094) or
- a range of comma-separated VLAN IDs (for example 1-20,30,40-50).

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create a port channel interface for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a port channel interface for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

Step 4 Hover your cursor over **Logical** and choose **Port Channel**.

Step 5 Click **Add**.

Step 6 In the **Create Port Channel** slide-in pane, complete the required configurations.

a) In the **Port Channel Number** field, enter the port channel number.

The valid range is from 1 to 64.

b) (Optional) In the **Description** field, enter a description.

You can enter up to 200 characters. Catalyst Center does not allow ? in the description.

c) Use the **Admin Status** toggle button to enable or disable the interface.
d) Use the **Layer 3 Address** toggle button to change the port channel type from Layer 2 to Layer 3 or Layer 3 to Layer 2.

Note Changing the port channel type removes the port members. You must reselect the port members.

e) Under **Port Members**, configure port members for the port channel type.

If you want to...	Then...
search for port members	in the **Search** field, enter either the partial or full name of the port member and press **Enter**.
add port members	use one of these options: • Click the plus icon next to the required port member. • Click the port member and click **Add Selected**. **Note** To select and add multiple port members, press **Shift**, click the port member, and click **Add Selected**.

If you want to...	Then...
remove port members	use one of these options: • Click the **X** icon next to the required port member. • Click the port member and click **Remove Selected**. **Note** To select and remove multiple port members, press **Shift**, click the port member, and click **Remove Selected**. • Click **Remove All** to remove all port members.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Create loopback interface for a Cisco Catalyst 9800 Series Wireless Controller

The loopback interface is used for management and routing purposes in a wireless controller.

Use this procedure to create loopback interface for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

Step 4 Hover your cursor over the **Logical** tab, click **Loopback**.

Step 5 Click **Add**.

Step 6 In the **Create Loopback** slide-in pane, complete these configurations.

a) Enter a unique number as **Loopback Number**, which is used to identify the loopback interface.

b) (Optional) In the **Description** field, enter a description.
c) (Optional) Use the **Admin Status** toggle button to enable or disable the selected interface.
d) (Optional) From the **VRF** drop-down list, choose a VRF so that the loopback interface is associated with the selected VRF table. This ensures that the traffic on the loopback interface is routed according to the routing table of the VRF.
e) Enable the **Relay Information Option**, so that the received DHCP packets do not set the gateway IP address (giaddr) field. This configuration is used in networks where the relay agent needs to provide additional information to the DHCP server without specifying a gateway IP address. The DHCP server can then use the information in the relay agent information option to assign IP addresses and other configuration parameters.
f) Under **IP Options**, choose the required options.
g) If you choose **IPv4**, configure these settings:

- From the **IPv4 Type** drop-down list, choose the type of the IP address.
- In the **IP address** field, enter the IPv4 address to be assigned to the loopback interface.
- In the **Subnet Mask** field, enter the subnet mask.
- (Optional) Check the **Secondary IP** check box to assign a secondary IP address to the loopback interface. Enter the **Secondary IP** address and **Secondary IP Mask**.

h) If you choose **IPv6**, configure these settings:

- Select at least one of these IPv6 configurations:
  - **DHCP**: Enables DHCPv6 for the loopback interface. If chosen, then you can optionally enable the **Rapid Commit**, for delegation of the prefix.
  - **Autoconfig**: Configures the loopback interface automatically. If selected, then select the auto configuration to be inserted from the **Autoconfig** drop-down list.
  - **Act as an IPv6 DHCP client**: Enables automatic assignment of the IPv6 address. If chosen, then enter the prefix name in the **Act as an IPv6 DHCP client** field.
- Under **Static lists**, configure the static list.

If you want to...	Then...
add a static list	1. Click **Add**. 2. From the **Static** drop-down list in the **Add Static List** dialog box, choose a static list. 3. Based on the static list, enter a valid IPv6 address in the corresponding field. 4. Click **Save**.
delete static lists	1. Check the check box next to the static lists that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure an Ethernet port for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

Step 4 In the **Ethernet** tab, click the radio button next to the Ethernet port that you want to configure.

Step 5 Hover your cursor over **Actions** and choose **Edit**.

Step 6 (Optional) In the **General** tab of the **Edit Ethernet Ports** slide-in pane, in the **Description** field, enter a description for the port.

Step 7 (Optional) In the **Advanced** tab, choose the inbound and outbound IPv4 and IPv6 ACLs from the corresponding drop-down lists.

To create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785.

To create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller

The Virtual Routing and Forwarding (VRF) interface is used for segmenting multiple routing table instances in a wireless controller.

Use this procedure to create VRF interface for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

Step 4 In the **VRF** tab, click **Add**.

Step 5 In the **Create VRF** slide-in pane, complete these configurations.

- Choose the protocols from these options: **IPv4**, **IPv6**, or **IPv4/IPv6**. The routing table is created based on the selected protocol.
- In the **VRF name** field, enter a name for the VRF.
- In the **Route Distinguisher** field, enter the route distinguisher details in the **ASN:nn** format. This is a unique ID that is used to distinguish between routes in different VRFs
- For the **Route-Target Import**, click **Add** to specify the route-target extended community attributes that the VRF should import. This allows the VRF to accept routes from other VRFs that have matching route-target attributes.
- For the **Route-Target Export**, click **Add** to specify the route-target extended community attributes that the VRF should export. This allows the VRF to advertise its routes to other VRFs with matching route-target attributes.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure the wireless management interface for a Cisco Catalyst 9800 Series Wireless Controller

The wireless management interface is used for all communications between the wireless controller and APs. A wireless controller has a single wireless management interface.

Use this procedure to configure the wireless management interface for a wireless controller and provision it.

Note Changing the interface or trustpoint causes APs to disconnect and disrupt clients.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **Interfaces**.

Step 4 Click the **Wireless** tab.

Step 5 (Optional) Complete these configurations.

a) From the **Interface Name** drop-down list, choose an interface.

To create an SVI interface, refer to Create an SVI profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 930. To create an Ethernet port, refer to Configure an Ethernet port for a Cisco Catalyst 9800 Series Wireless Controller, on page 939.

b) In the **Trustpoint** field, enter the wireless management trustpoint name.
c) In the **NAT IPv4/IPv6 Server Address** field, enter the NAT IP address.
d) Use the toggle buttons to enable or disable these configurations:

- **Enable NAT on L3 Interface Cache**: Enable or disable Network Address Translation (NAT) for Layer 3 interface cache data.
- **Private IP Discovery**: Enable or disable the option to allow the wireless controller to detect and log private IP addresses associated with client devices.
- **Public IP Discovery**: Enable or disable the option to allow the wireless controller to detect and log public IP addresses associated with client devices.

Step 6 Under **Controller Management Security**, complete these configurations:

- In the **SSC Authentication Token** field, enter the Secure Socket Communications (SSC) token used for secure management communication with the wireless controller.

Note Ensure that this token is kept confidential and matches the expected value on peer devices or management systems.

- From the **SSC Auth Token Type** drop-down list, choose the encryption or hashing method used to store and transmit the SSC authentication token.

Note If you change the token type, you may need to update tokens on all connected systems.

Step 7 Under **SSC Trust Hashes**, configure SSC trust hashes.

If you want to...	Then...
Add an SSC trust hash	**a.** Click **Add**. **b.** In the **SSC Certificate Fingerprint** field of the **Add SSC Trust Hash** dialog box, enter the fingerprint or hash of the SSC used by an AP for secure communication with the wireless controller. **c.** Click **Save**.
Edit an SSC trust hash	**a.** Check the check box next the SSC trust hash that you want to edit. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Edit the configuration. **d.** Click **Save**.
Delete SSC trust hashes	**a.** Check the check box for the SSC trust hashes that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure discovery protocols for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure discovery protocols for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 2** and click **Discovery Protocols**.

Step 4 Under **CDP**, complete these configurations.

a) Use the **CDP Status** toggle button to enable or disable Cisco Discovery Protocol (CDP).

If you enable CDP, enter data in these fields.

- **Hold Time**: enter the hold time, in seconds, to be sent in CDP packets.

  The valid range is from 10 to 255.

- **Timer**: enter the rate, in seconds, at which CDP packets are sent.

  The valid range is from 5 to 254.

b) From the **CDP Advertisement Version** drop-down list, choose the required version.

Step 5 Under **LLDP**, complete these configurations.

a) Use the **LLDP Status** toggle button to enable or disable the Link Layer Discovery Protocol (LLDP).
b) (Optional) Add the type, length, and value (TLV) using one of these methods.

- Click the plus icon next to the required TLV.
- Click the required TLV and click **Add Selected**.

  To choose multiple TLVs, press **Shift**, click the TLV, and click **Add Selected**.

- To add all the TLVs, click **Add All**.

  You can use the **Search** field to filter the TLVs.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Network settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device network settings for a Cisco Catalyst 9800 Series Wireless Controller.

Configure DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure DNS-based hostname-to-address translation for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **DNS**.

Step 4 Use the **DNS Loopback** toggle button to enable or disable DNS-based address to hostname translation

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

What to do next

If you enable DNS loopback, in the **DNS** table, you can add, edit, or delete DNS servers. To add a DNS server, see Add a DNS server for DNS loopback, on page 945.

Add a DNS server for DNS loopback

Use this procedure to add a DNS server for DNS-based hostname to address translation for a Cisco Catalyst 9800 Series Wireless Controller.

If you enable DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller, you must add at least one DNS server. To configure DNS loopback, see Configure DNS loopback for a Cisco Catalyst 9800 Series Wireless Controller, on page 944.

Note A DNS IPv6 server address created in the long format is converted to the short format after device resync.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **DNS**.

Step 4 In the **DNS** table, click **Add**.

Step 5 In the **Create DNS** slide-in pane, complete these configurations:

a) (Optional) To enable VRF, check the **VRF** check box.

b) If you enable VRF, from the **VRF Name** drop-down list, choose a VRF.

Note When VRF is enabled, Catalyst Center does not support the VRF **None**.

To create a VRF interface, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

c) Configure DNS servers.

If you want to...	Then...
add a DNS server	1. Click **Add**. 2. In the **DNS Server(IPv4 / IPv6)** field of the **Add DNS Server(IPv4 / IPv6)** dialog box, enter a valid IPv4 or IPv6 address of the DNS server. 3. Click **Save**.
delete DNS servers	1. Check the check box next to the DNS servers that you want to delete. 2. Hover your cursor over **Actions** and select **Delete**. 3. In the dialog box, click **Yes**.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create an IPv4 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv4 DHCP pool for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **DHCP Pools**.

Step 4 Hover your cursor over **DHCP Pools** and choose **IPv4**.

Step 5 Click **Add**.

Step 6 In the **General** tab of the **Create DHCP Pools** slide-in pane, complete these configurations.

a) In the **DHCP Pool Name** field, enter a unique name for the DHCP pool.

The DHCP pool name can contain up to 236 characters. Catalyst Center does not support ? or spaces in the DHCP pool name.

b) (Optional) Check the **VRF** check box to enable VRF.

If you enable VRF, from the **VRF Name** drop-down list, choose a VRF to associate with the DHCP pool.

c) In the **Network** field, enter a valid network IP address.

d) From the **Subnet Mask** drop-down list, choose a subnet mask.

e) From the **Lease** drop-down list, choose an option for lease expiry.

If you chose the **User Defined** option, enter data in these fields.

- **Days** (the valid range is from 0 to 365)
- **Hours** (the valid range is from 0 to 23)
- **Minutes** (the valid range is from 0 to 59)

Step 7 (Optional) In the **Advanced** tab, complete these configurations.

a) In the **Domain** field, enter a domain name.

Domain names can contain up to 255 characters for wireless controllers running Cisco IOS XE Release 17.15.1 or later. Catalyst Center does not support ? or spaces in the domain name.

b) (Optional) Under **Default Router**, configure default routers.

If you want to...	Then...
add a default router	1. Click **Add**. 2. In the **Default routers** field of the **Add Default Router(s)** dialog box, enter the default router IP address. 3. Click **Save**. **Note** The default router must be in the same subnet as the DHCP pool.
delete default routers	1. Check the check box next to the default routers that you want to delete. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

c) (Optional) Under **DNS Server**, configure DNS servers.

If you want to...	Then...
add a DNS server	1. Click **Add**. 2. In the **DNS Server List** field of the **Add DNS Server** dialog box, enter the DNS server IPv4 address. 3. Click **Save**.

If you want to...	Then...
delete DNS servers	1. Check the check box next to the DNS servers that you want to delete. 2. Hover your cursor over **Actions** and click **Delete**. 3. In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an IPv6 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an IPv6 DHCP pool for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **DHCP Pools**.

Step 4 Hover your cursor over **DHCP Pools** and choose **IPv6**.

Step 5 Click **Add**.

Step 6 In the **DHCP Pool Name** field of the **Create DHCP Pools** slide-in pane, enter a unique name for the DHCP pool.

The DHCP pool name can contain up to 232 characters. Catalyst Center does not support ? or spaces in the DHCP pool name.

Step 7 (Optional) Under **Domain Names**, configure domain names.

If you want to...	Then...
add a domain name	**a.** Click **Add**. **b.** In the **Domain Name** field of the **Add Domain Names** dialog box, enter the domain name. The domain name can contain up to 225 characters. **c.** Click **Save**.
delete domain names	**a.** Check the check box next to the domain names that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Under **DNS Server**, configure DNS servers.

If you want to...	Then...
add a DNS server	**a.** Click **Add**. **b.** In the **DNS Server List** field of the **Add Domain Names** dialog box, enter the DNS server IPv6 address. **c.** Click **Save**.
delete DNS servers	**a.** Check the check box next to the DNS servers that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 9 Under **IPV6 Address Allocation**, configure IPv6 address allocation.

If you want to...	Then...
add an IPv6 address	**a.** Click **Add**. **b.** In the **IPv6 Address** field of the **Add IPV6 Address Allocation** dialog box, enter the IPv6 address. **c.** Click **Save**.
delete IPv6 addresses	**a.** Check the check box next to the IPv6 addresses that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Configure DHCP persistence for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure DHCP persistence for a Cisco Catalyst 9800 Series Wireless Controller and provision the configuration.

Before you begin

Ensure that you have already created the DHCP pools.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **DHCP Pools**.

Step 4 Click the **DHCP Persistence** tab. Select the interface to configure DHCP persistence.

Step 5 Hover your cursor over **Action** and click **Edit**.

Alternatively, click the interface name.

Step 6 In the **Edit DHCP Persistence** slide-in pane, configure these parameters:

- **Interface**: Displays the client interface for which the IP address should be assigned.
- **Pool Name**: Choose the DHCP pool name from the drop-down list. By default, the DHCP pool **None** is selected.

  To create a DHCP pool, see Create an IPv4 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller, on page 946 and Create an IPv6 DHCP pool for a Cisco Catalyst 9800 Series Wireless Controller, on page 948.

Note To change the DHCP pool name, first choose the DHCP pool **None** and provision the configuration. After the provisioning is completed, choose the required DHCP pool.

- **Reserved IP Address**: Enter the reserved IP address.

  This IP address ensures that these IP addresses are not dynamically assigned to other devices.

Note This field is disabled when the DHCP pool **None** is selected.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure HTTP and HTTPS for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure HTTP and HTTPS for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **HTTP/HTTPS**.

Step 4 Check the required check boxes to enable the corresponding configurations.

- **HTTP Access**: enable the HTTP server.

  If you check this check box, in the **HTTP Port** field, enter the HTTP port number.

  The valid values are either 80 or any number from 1024 to 65535.

Note The HTTP and HTTPS port numbers must be different. To switch to a port that is already in use for HTTPS, provision a new port for HTTPS and then use the port for HTTP.

For example, if HTTPS is configured to use port 1028 and you want HTTP to use port 1028, first change the HTTPS port to a different number and provision the configuration, and then assign port 1028 to HTTP.

- **HTTPS Access**: enable the HTTPS secure server.

  If you check this check box, in the **HTTPS Port** field, enter the HTTPS port number.

  The valid values are either 443 or any number from 1025 to 65535.

Note The HTTP and HTTPS port numbers must be different. To switch to a port that is already in use for HTTP, provision a new port for HTTP and then use the port for HTTPS.

For example, if HTTP is configured to use port 1026 and you want HTTPS to use port 1026, first change the HTTP port to a different number and provision the configuration, and then assign port 1026 to HTTPS.

- **Personal Identity Verification**: enable personal identity verification.

Note Configure the trustpoint, CA server certificate on the wireless controller. Ensure that the client certificate is signed by the CA server on the browser. Otherwise, access to the wireless controller UI is not available.

  If you enable personal identity verification, you can optionally check the **Personal Identity Verification Authorization only** check box to set the verification for only the web UI.

Step 5 From the **Authentication** drop-down list, choose an authentication method.

If you chose **aaa**, from these drop-down lists, you can optionally choose the required options.

- **Authorization List** (to create an authorization method list, see Create an authorization method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 777)
- **Authentication List** (to create an authentication method list of the type **LOGIN**, see Create an authentication method list for a Cisco Catalyst 9800 Series Wireless Controller, on page 776)

Step 6 (Optional) Under **HTTP Proxy Configuration**, enter data in both these fields.

- **Client Proxy Server**: enter the client proxy server.

  You can enter an IPv4 address, IPv6 address, or host name.

- **Client Proxy Port**: enter the client proxy port.

The valid range is from 1 to 65535.

Note If you enter data in one of these fields, you must also enter data in the other field. Catalyst Center supports the combined length of up to 215 characters for both fields.

Step 7 Under **HTTP Trustpoint**, use the **Enable TrustPoint** toggle button to enable or disable the HTTP trustpoint.

If you enable HTTP trustpoint, from the **Secure Trustpoint** drop-down list, choose a secure server certificate trustpoint.

Note Changes to the secure trustpoint settings in the HTTP interface can disrupt access to the wireless controller UI, potentially affecting the management capabilities.

Step 8 Under **Timeout Policy**, enter data in these fields:

- **HTTP Timeout-policy (secs)**: enter the idle timeout of HTTP server connection in seconds.

  The valid range is from 1 to 600.
- **Session Idle Timeout(secs)**: enter the HTTP server session idle timeout in seconds.

  For wireless controllers running Cisco IOS XE Release 26.2.1 or later, the valid range is from 180 to 14400. For wireless controllers running versions earlier than Cisco IOS XE Release 26.2.1, the valid range is from 180 to 1200.
- **Server Life Time (secs)**: enter the lifetime of an HTTP server connection in seconds.

  The valid range is from 1 to 86400.
- **Max number of requests**: enter the maximum number of requests allowed on an HTTP server connection.

  The valid range is from 1 to 86400.

Step 9 Click **Review and Provision**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Configure general SNMP parameters for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the general SNMP parameters for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

Step 4 (Optional) In the **General** tab, enter data in these fields.

- **System Location**: enter the location of the device.

  The system location can contain up to 234 characters. Catalyst Center does not support ? in the system location.

- **System Contact**: enter the contact details of the device administrator.

  The contact details can contain up to 235 characters. Catalyst Center does not support ? in the contact details.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Configure SNMP wireless traps for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure SNMP wireless traps for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

Step 4 Click the **Wireless Traps** tab.

Step 5 Use the **Enable** toggle button under each area to enable or disable the corresponding traps.

- **General Controller**
- **Mesh**
- **RF**
- **Rogue**
- **RRM**
- **Wireless Client**
- **Wireless Mobility**

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Add an SNMP community string for a Cisco Catalyst 9800 Series Wireless Controller

An SNMP community string is a password that is used to authenticate access to the managed devices. It can also be used for device discovery.

Note If an SNMP community string used for device discovery is deleted, the device enters into an Unmanaged state on Catalyst Center.

Use this procedure to add an SNMP community string for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

Step 4 Click the **Community Strings** tab.

Step 5 Click **Add**.

Step 6 In the **Community Name** field of the **Add Community String** slide-in pane, enter the SNMP community string.

SNMP community string is a password to authenticate access to the managed devices. The string can contain up to 128 characters. Catalyst Center does not support ?, backslash (\), and spaces in the string.

Step 7 From the **Access Mode** drop-down list, choose a mode in which the SNMP management station can retrieve information from the device.

- **Read Only**: view or retrieve information from the network device.
- **Read/Write**: view information and modify device settings and configurations.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create SNMPv3 user group for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create SNMPv3 user group for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

Step 4 Click the **V3 User Groups** tab.

Step 5 Click **Add**.

Step 6 In the **Group Name** field of the **Create V3 User Groups** slide-in pane, enter a unique name for the SNMPv3 user group.

The user group name can contain up to 32 characters.

Step 7 Under **Security Level**, configure the level of the security for the user group.

If you want to...	Then...
add a security level	**a.** Click **Add**. **b.** From the **Security Level** drop-down list in the **Add Security Level** dialog box, choose a security level. • **AUTH**: Messages are authenticated but not encrypted. • **NOAUTH**: No security applied. • **PRIV**: Messages are authenticated and encrypted. **Note** Security level types must be unique in a user group. **c.** (Optional) In the **Read View** field, specify the read view for the group **d.** (Optional) In the **Write View** field, specify the write view for the group.
edit a security level	**a.** Check the check box for the security level. **b.** Hover your cursor over **Actions** and choose **Edit**. **c.** Update the required configuration. **d.** Click **Save**.
delete security levels	**a.** Check the check box security levels that you want to delete. **b.** Hover your cursor over **Actions** and choose **Delete**. **c.** In the dialog box, click **Yes**.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Create an SNMPv3 user for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an SNMPv3 user for a wireless controller and provision it. SNMPv3 provides enhanced security for network management by supporting authentication and privacy.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.

c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.

b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

Step 4 Click the **V3 Users** tab.

Step 5 Click **Add**.

Step 6 In the **Create V3 User Groups** slide-in pane, complete these configurations:

a) In the **Username** field, enter a unique name for the SNMPv3 user.

The user group name can contain up to 32 characters.

b) From the **Group Name** drop-down list, choose an SNMPv3 user group.

To create an SNMPv3 user group, see Create SNMPv3 user group for a Cisco Catalyst 9800 Series Wireless Controller, on page 956.

c) From the **Security Mode** drop-down list, choose a security level for authentication and privacy.

If you choose...	Then...
AuthPriv	• From the **Privacy Protocol** drop-down list, choose a protocol for data encryption. • From the **Privacy Encryption** drop-down list, choose an encryption method for the privacy password. **Note** To use encryption types **6** or **7**, ensure that the device is configured to accept plain-text passwords, or provide the preencrypted password. Otherwise, choose encryption type **0**. • In the **Privacy Password** field, enter the privacy password.

If you choose...	Then...
AuthPriv or **AuthNoPriv**	• From the **Authentication Protocol** drop-down list, choose a protocol for authentication. If you choose **SHA2**, from the **Authentication Algorithm** drop-down list, choose the bit length for SHA-2 authentication algorithm. • From the **Authentication Encryption** drop-down list, choose an encryption method for the authentication password. **Note** To use encryption types **6** or **7**, ensure that the device is configured to accept plain-text passwords, or provide the preencrypted password. Otherwise, choose encryption type **0**. • In the **Authentication Password** field, enter the authentication password. • (Optional) From the **ACL IPv6** drop-down list, choose an IPv6 ACL. To create an IPv6 ACL, see Create an IPv6 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 792.
AuthPriv, **AuthNoPriv**, or **NoAuthNoPriv**	(Optional) From the **ACL IPv4** drop-down list, choose an IPv4 ACL. To create an IPv4 ACL, see Create an IPv4 ACL for a Cisco Catalyst 9800 Series Wireless Controller, on page 785.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

The **V3 Users** table shows only the SNMPv3 users with encrypted passwords.

Create an SNMP host for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an SNMP host for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **SNMP**.

Step 4 Click the **Hosts** tab.

Step 5 Click **Add**.

Step 6 In the **IP Address** field of the **Create SNMP Host** slide-in pane, enter the IP address of the host.

Step 7 From the **Version** drop-down list, choose an SNMP version to send the trap.

If you choose...	Then...
V1 or **V2C**	from the **Community String** drop-down list, choose an SNMP community string. To add a community string, refer to Add an SNMP community string for a Cisco Catalyst 9800 Series Wireless Controller, on page 955.
V3	complete these configurations: • In the **V3 User** field, enter the user name for SNMPv3 authentication and encryption. • From the **Security Level** drop-down list, choose a security level.

Step 8 (Optional) In the **UDP Port** field, enter the number for the SNMP destination port.

The valid range is from 0 to 65535. The default value is 162.

Step 9 From the **Type** drop-down list, choose the type of SNMP notifications.

- **traps**: SNMP notifications are unacknowledged.
- **informs**: SNMP notifications are acknowledged.

Step 10 Click **Review and Provision**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Create an NTP server profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a Network Time Protocol (NTP) server profile for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **NTP**.

Step 4 In the **NTP** tab, click **Add**.

Step 5 In the **Host Name** field of the **Create NTP Server Profile** slide-in pane, enter the host name.

You can enter an IPv4 address, IPv6 address, or a Fully Qualified Domain Name (FQDN).

Step 6 (Optional) Check the **Prefer** check box to use this NTP server profile by default.

Step 7 From the **IP for DNS Resolution** drop-down list, choose the type of IP address used for Domain Name System (DNS) resolution.

Step 8 From the **Source Address** drop-down list, choose an interface that is used to communicate with the NTP server.

If you chose...	Then...
VLAN	from the **VLAN** drop-down list, choose a VLAN to communicate with the NTP server.
Interface	from the **Interface** drop-down list, choose the interface that is used to communicate with the NTP server.

Step 9 (Optional) Check the **Enable Authentication** check box to enable authentication against the NTP server.

If you check this check box, from the **Key** drop-down list, choose a key index that is used for authentication.

To create an authentication key profile, see Create an authentication key profile for a Cisco Catalyst 9800 Series Wireless Controller, on page 962.

Step 10 (Optional) Check the **VRF** check box to configure NTP servers for each VRF to ensure accurate time synchronization within isolated routing domains, enhancing network reliability and event logging for specific segments.

If you check this check box, based on the IP address option that you choose for DNS resolution choose a VRF interface from the corresponding drop-down list. To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

Step 11 Click **Review and Provision**.

Step 12 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 13 On the **Tasks** window, monitor the task deployment.

Create an authentication key profile for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create an authentication key profile to authenticate against an NTP server for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Network Settings** and click **NTP**.

Step 4 Click the **Authentication Keys** tab.

Step 5 Click **Add**.

Step 6 In the **Authentication Key Number** field of the **Create Authentication Key** slide-in pane, enter a unique authentication key number.

The valid range is from 1 to 4294967295.

Step 7 In the **Authentication Key** field, enter an authentication key for MD5 authentication.

The authentication key can contain up to 32 characters. Catalyst Center does not support ? and spaces in the authentication key.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device Layer 3 configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Create a static route for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to create a static route for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Layer 3** and click **Routing**.

Step 4 In the **Static** tab, hover your cursor over **Add** and choose the required static route option.

Step 5 If you chose **IPv4**, in the **Create Static Route** slide-in pane, complete these configurations.

a) In the **Prefix** field, enter the static route prefix.
b) In the **Prefix Mask** field, enter the static route prefix mask.
c) (Optional) Check the **VRF** check box to enable Virtual Routing and Forwarding (VRF).

   If you check this check box, from the **VRF Name** drop-down list, choose a VRF. To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

d) (Optional) Check the **DHCP** check box to obtain the default gateway from DHCP.

   If you check this check box, in the **Metric** field, enter a value.

   The valid range is from 1 to 255. The default value is 1.

e) (Optional) Under **Route Path List**, configure route path lists.

If you want to...	Then...
add a route path list	1. Click **Add**. 2. From the **Route Path** drop-down list in the **Add Route Path List** dialog box, choose a route path. If you chose **Interface**, from the **Interface** drop-down list, choose an interface. 3. In the **Next Hop IP** field, enter the next hop IP address. If you chose **Interface**, this field is optional. 4. In the **Metric** field, enter a value. The valid range is from 1 to 255. The default value is 1. 5. Click **Save**.
delete route path lists	1. Check the check box next to the required route paths. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

Step 6 If you chose **IPv6**, in the **Create Static Route** slide-in pane, complete these configurations.

a) In the **Prefix** field, enter the static route IPv6 prefix.

b) In the **Prefix Length** field, enter the static route prefix length.

c) (Optional) Check the **VRF** check box to enable Virtual Routing and Forwarding (VRF).

If you check this check box, from the **VRF Name** drop-down list, choose a VRF. To create a VRF, see Create VRF interface for a Cisco Catalyst 9800 Series Wireless Controller, on page 940.

d) (Optional) Under **Route Path List**, configure route path lists.

If you want to...	Then...
add a route path list	1. Click **Add**. 2. From the **Route Path** drop-down list in the **Add Route Path List** dialog box, choose a route path. If you chose **Interface**, from the **Interface** drop-down list, choose an interface. 3. In the **Next Hop IP** field, enter the next hop IP address. If you chose **Interface**, this field is optional. 4. (Optional) In the **Administrative Distance** field, enter a value. The valid range is from 1 through 254. The default value is 1. 5. Click **Save**.

If you want to...	Then...
delete route path lists	1. Check the check box next to the required route paths. 2. Hover your cursor over **Actions** and choose **Delete**. 3. In the dialog box, click **Yes**.

Step 7 Click **Review and Provision**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller

Use this section for information about per-device administrative configurations for a Cisco Catalyst 9800 Series Wireless Controller.

Configure device administration settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the device administration settings for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Administration** and click **Device**.

Step 4 In the **General** tab, complete these configurations:

- Use the **IP Routing** toggle button to enable or disable IP routing.

- In the **Host Name** field, enter the host name.

  The host name can contain uppercase and lowercase letters, numbers, hyphens (-), underscores (_), and periods (.). The host name must not contain only numbers.

- (Optional) In the **Banner** field, enter the required data.

Step 5 Click **Review and Provision**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Configure device FTP/SFTP/TFTP settings for a Cisco Catalyst 9800 Series Wireless Controller

In a network, you can ensure secure transfer of files between devices by configuring one of these transfer protocols:

- File Transfer Protocol (FTP): Used for transferring files between a client and a server over a network.
- Secure File Transfer Protocol (SFTP): Uses Secure Shell (SSH) for encrypted file transfers.
- Trivial File Transfer Protocol (TFTP): A simpler, lightweight protocol for transferring files, often used for network booting or firmware upgrades.

Use this procedure to configure the FTP, SFTP, and TFTP settings for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Administration** and click **Device**.

Step 4 Click the **FTP/SFTP/TFTP** tab.

Step 5 Under **FTP Settings**, complete these configurations:

- From the **Source Interface** drop-down list, choose the source interface.

- **Username**: Enter a user name for the FTP connection.

  The user name can contain up to 237 characters. Catalyst Center does not support ? and spaces in the user name.

- **Password**: Enter a password for the FTP connection.

  The password can contain up to 25 characters. It must contain at least one alphanumeric character. Catalyst Center does not support ? in the password.

Step 6 Under **SFTP Settings**, from **Source Interface** drop-down list, choose an interface.

Step 7 Under **TFTP Settings**, from the **Source Interface** drop-down list, choose an interface.

Step 8 Click **Review and Provision**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure user administration settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the user administration settings for a wireless controller and provision the configuration.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Administration** and click **User Administration**.

Step 4 Click **Add**.

Step 5 In the **Create User Administration** slide-in pane, configure the parameters to define the user role and privilege.

a) **User Name**: Enter a unique user name for the new account.

   The name can contain up to 64 characters. Catalyst Center does not support ? in the user name.

b) **Policy**: Choose a password policy from the drop-down list. This policy is associated with the user.
c) **Advanced Mode**: Toggle this option to enable the privilege level to the advanced mode.

d) **Privilege**: Choose the user privilege level based on the mode. If you have not enabled the **Advanced** mode, then the privilege is set for the basic mode.

e) If you choose the basic mode, these privilege options are available:

- **Admin**: Users have access to all the sections in the GUI.
- **Read Only**: Users have access only to the dashboard and monitoring sections.
- **No Access**: Users cannot access the GUI.
- **Lobby Admin**: Users who can create only guest user accounts.

Note To change the privilege from Lobby Admin to another role or vice versa, delete the existing entry and add a new entry with the required privilege.

f) If you choose the advanced mode, choose the privilege level from 0 to 15.

- Privilege 15 is an admin user.
- Privileges 1 to 14 are considered as read-only users.
- Privilege 0 has no access.

g) **Password**: Enter a password for the user account and re-enter it for confirmation in the **Confirm Password** field.

The password can contain up to 127 characters. The password in the **Confirm Password** field must match the password in the **Password** field.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure AP upgrade settings for a Cisco Catalyst 9800 Series Wireless Controller

Use this procedure to configure the AP upgrade settings for a wireless controller and provision it.

Procedure

Step 1 Navigate to the required wireless controller in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.

b) From the top-left corner, click **Global** and choose an area, building, or floor.
c) Click the **Wireless Controllers** device family button to display the list of available wireless controllers.

Step 2 Open the device details window for the required wireless controller.

a) Click the device name.
b) In the dialog box with the device information, click **View Device Details** to open the device details window.

Step 3 In the **Configuration** tab, expand **Administration** and click **AP Upgrade Configuration**.

Step 4 From the **AP Upgrade Percentage per Iteration** drop-down list, choose the required option for AP upgrade percentage per iteration or AP upgrade mode.

These options are available:

- Staggered upgrade: to upgrade the APs associated with the wireless controller in batches based on the selected percentage.
- One-time upgrade: to upgrade all the APs associated with the wireless controller in a single iteration.
- Serial upgrade: to upgrade one AP associated with the wireless controller at a time.

You can choose a staggered upgrade percentage, one-time upgrade, or serial upgrade of the APs associated with the wireless controller.

Step 5 Use these check boxes to enable or disable the corresponding settings:

- **Client Steering**: Steer clients away from AP during the upgrade.
- **Client Deauthentication**: Deauthenticate clients connected to the AP during the upgrade before it reloads.

Step 6 Click **Review and Provision**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Inter-Release Controller Mobility introduction

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different Cisco Wireless Controllers with different software versions.

Catalyst Center supports the guest anchor feature for device combinations, including:

- Configuration of a Cisco AireOS controller as a foreign controller with a Cisco AireOS controller as an anchor controller.

- Configuration of a Cisco AireOS controller as a guest anchor controller with a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller.
- Configuration of a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller with a Cisco Catalyst 9800 Series Wireless Controller as an anchor controller.

Configuring IRCM on controller devices has limitations, including:

- Configuration of a Cisco AireOS controller as a foreign controller and Cisco Catalyst 9800 Series Wireless Controller as an anchor controller is not supported.
- Configuration of a fabric guest anchor is not supported.
- Only guest SSID is supported.
- Broadcast of a nonguest anchor SSID in guest anchor mode is not supported.

Guest anchor configuration and provisioning process

Use this procedure to configure a guest anchor Cisco Wireless Controller.

Procedure

Step 1 Design a network hierarchy, with sites, buildings, floors, and so on. For more information, see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

Step 2 Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see Configure global network servers, on page 321 and Add Cisco ISE or other AAA servers, on page 319.

Step 3 Create SSIDs for a guest wireless network with external web authentication and central web authentication along with configuring Cisco Identity Services Engine. For more information, see Create SSIDs for a guest wireless network, on page 366.

Step 4 Discover the wireless controller using the Cisco Discovery Protocol (CDP) or an IP address range, and make sure that the devices are in the **Devices** > **Inventory** window and in the **Managed** state. For more information, see Discovery overview, on page 55.

Step 5 Provision a foreign wireless controller as the active main wireless controller. See Provision a Cisco AireOS Controller, on page 620.

Note If you choose a site with multiple network profiles while provisioning a foreign wireless controller, ensure that the total number of anchor groups for the network profiles is three or less.

Step 6 Choose the role for the wireless controller as guest anchor and provision the guest anchor controllers. For more information, see Provision a Cisco AireOS Controller, on page 620.

Note

- You must choose the same site as the managed AP location for the anchor wireless controller as specified for the SSID.
- If you modify the interface configuration for the anchor wireless controller, you must reprovision it.

Step 7 Configure device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, Add global SNMPv3 credentials, on page 325, and Add global HTTPS credentials, on page 327.

Prerequisites for configuring IRCM on a Cisco controller device

- Discover the Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

  You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations of network devices.

  For more information, see Discover your network using CDP, on page 66 or Discover your network using an IP address range or CIDR, on page 68.

- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

  To create a new network hierarchy, see Create, edit, and delete a site, on page 240 and Add, edit, and delete a building, on page 242.

- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

  For more information, see Work with APs on a floor map, on page 256.

- Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

  For more information, see Network settings overview, on page 317, Configure global network servers, on page 321, and Add AAA server.

- Create SSIDs for a guest wireless network.

  For more information, see Create SSIDs for a guest wireless network, on page 366.

- The WLAN profile name of the foreign controller and anchor controller should be the same for mobility.

Configuring IRCM on a Cisco AireOS Controller and a Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Ensure the prerequisites for configuring IRCM are met. For more information, see Prerequisites for configuring IRCM on a Cisco controller device, on page 971.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window display with the discovered devices listed.

Step 2 Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision as a foreign controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision**.

Step 4 In the **Assign Site** window, click **Choose a Site** to assign a site for the Catalyst 9800 Series Wireless Controller device.

Step 5 In the **Add Sites** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

Step 6 Click **Save**.

Step 7 Click **Apply**.

Step 8 Click **Next**.

Step 9 Select a role for the Catalyst 9800 Series Wireless Controller as **Active Main WLC**.

Step 10 For an active main wireless controller, you need to configure interface and VLAN details.

Step 11 Under the **Assign Interface** area, do these steps:

a) **VLAN ID**: Enter a value for the VLAN ID.
b) **IP Address**: Enter the interface IP address.
c) **Gateway IP Address**: Enter the gateway IP address.
d) **Subnet Mask (in bits)**: Enter the interface net mask details.

Note Assigning an IP address, gateway IP address, and subnet mask is not required for the Catalyst 9800 Series Wireless Controller.

Step 12 Click **Next**.

Step 13 In the **Summary** window, review the configuration settings.

Step 14 Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller as a foreign controller.

Step 15 On the **Devices** > **Inventory** window, check the check box next to the Cisco AireOS Controller that you want to provision as a guest anchor controller.

Step 16 Repeat Step 3 through Step 8.

Step 17 Select a role for the Cisco AireOS Controller as **Guest Anchor**.

Step 18 For a guest anchor wireless controller, you need to configure the interface and VLAN details.

Step 19 Repeat Step 11 through Step 14.

Prerequisites for provisioning a Meraki device

- Integrate the Meraki dashboard with Catalyst Center. See Integrate the Meraki dashboard, on page 148.
- Create the SSID. See Create SSIDs for an enterprise wireless network, on page 351.

Note The Meraki dashboard supports these types of SSIDs:

- Open: This SSID corresponds to Open in the Meraki dashboard.
- WPA2 Personal: This SSID corresponds to the preshared key with WAP2 in the Meraki dashboard.
- WPA2 Enterprise: This SSID corresponds to WAP-2 Encryption with Meraki authentication or My Radius server in the Meraki dashboard. If you have defined AAA or Cisco ISE servers for client and endpoint authentication at the building level in Catalyst Center, the configuration is provisioned to **my Radius server** in the Meraki dashboard. Otherwise, **Meraki Radius** is used for authentication by the Meraki devices.

For every SSID, you can choose an interface name. If you choose the **Management** interface in Catalyst Center and the VLAN ID is 0, the configuration is not supported in the Meraki dashboard and VLAN tagging is disabled in the Meraki dashboard. If you create a custom interface for the SSID in Catalyst Center, an AP tag is created with the custom interface name and VLAN ID in the Meraki dashboard.

- Create the network profile and assign it to the sites for which the SSID is provisioned.

Note The Network Hierarchy **Sites** > **Buildings** in Catalyst Center corresponds to **Organization** > **Network** in the Meraki dashboard. We recommend that you choose **Buildings** in the **Add Sites to Profile** window in the workflow.

Note Catalyst Center creates the Meraki network and provisions the SSIDs to the network. The Meraki dashboard provisions the Meraki network configuration to the Meraki devices.

Provision a Meraki device

This procedure explains how to provision SSIDs for Cisco Meraki devices managed by a Meraki dashboard.

Before you begin

Ensure the prerequisite is met. For more information, see Prerequisites for provisioning a Meraki device, on page 973.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

Step 2 To view the Meraki dashboard, expand the **Global** site in the left pane, and choose a building.

All Meraki dashboards available in the chosen building display.

Step 3 Check the check box next to the Meraki dashboard name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window displays, which is where you can view the Meraki dashboard and the associated building.

Step 5 To change the associated building, click **Choose a site**.

Step 6 In the **Choose a site** window, select a building and click **Save**.

Step 7 Click **Next**.

The **Configuration** window displays. You can view the managed building in the primary location.

Step 8 Click **Select Secondary Managed AP Locations** to choose the secondary managed location for the Meraki dashboard.

Step 9 In the **Managed AP Location** window, check the check box next to the building name.

Step 10 Click **Save**.

Step 11 Click **Next**.
In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Note Meraki deployment supports a maximum of 15 SSIDs in each network.

Step 12 Click **Deploy**.

Step 13 In the **Provision Devices** window, do these steps to preview the CLI configuration:

a) Click the **Generate Configuration Preview** radio button.
b) In the **Task Name** field, enter a name for the CLI preview task, and click **Apply**.
c) In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Tasks** window, click the menu icon and choose **Activities** > **Tasks**.

d) In the **Tasks** window, click the CLI preview task for which you submitted the configuration preview request.
e) View the CLI configuration details, and click **Deploy**.
f) To immediately deploy the device, click the **Now** radio button, and click **Apply**.

g) To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
h) In the **Information** dialog box, do these steps:
   1. Click **Yes** if you want to delete the CLI preview task from the **Tasks** window.
   2. Click **No** if you want to retain the task in the **Tasks** window.

Note The CLI task will be marked as completed in the **Tasks** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Note After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

The **Provision Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

Provision remote teleworker devices

These topics explain the components of remote teleworker sites and the procedure for provisioning remote teleworker devices.

Remote teleworker deployment overview

Deployment components

The Cisco remote teleworker deployment is built around three main components: Cisco wireless controllers, Cisco OfficeExtend access points (APs) and a Corporate firewall. These models are supported in this deployment:

- **Wireless Controllers**: Cisco 5520 Wireless Controller, Cisco 8540 Wireless Controller, Cisco 3504 Wireless Controller[4], Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller, and Cisco Catalyst 9800-L Wireless Controller.
- **Access Points**: Cisco Aironet 1815T (Teleworker) Access Point, Cisco Aironet 1815I Access Point, Cisco Aironet 1815W Access Point, Cisco Aironet 1840I Access Point, Cisco Aironet 2800 Series Access Points, Cisco Aironet 3800 Series Access Points, Cisco Aironet 4800 Series Access Points, Cisco Catalyst 9115 Access Point, Cisco Catalyst 9120 Access Point, and Cisco Catalyst 9130 Access Point.

[4] Supported with Cisco Aironet 1815 Teleworker Access Point only.

Cisco Wireless Controllers

Cisco controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco APs to support business-critical wireless applications for teleworkers. Controllers provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

To allow users to connect their corporate devices to the organization's on-site wireless network, the remote teleworking solution offers the same wireless Secure Set Identifiers (SSIDs) at a teleworker's home as those that support data and voice inside the organization.

Cisco OfficeExtend Access Points

APs cannot act independently of controllers. As an AP communicates with the controller resources, it downloads its configuration and synchronizes its software or firmware image, if required. The AP establishes a secure Datagram Transport Layer Security (DTLS) connection to the controller, which offers remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

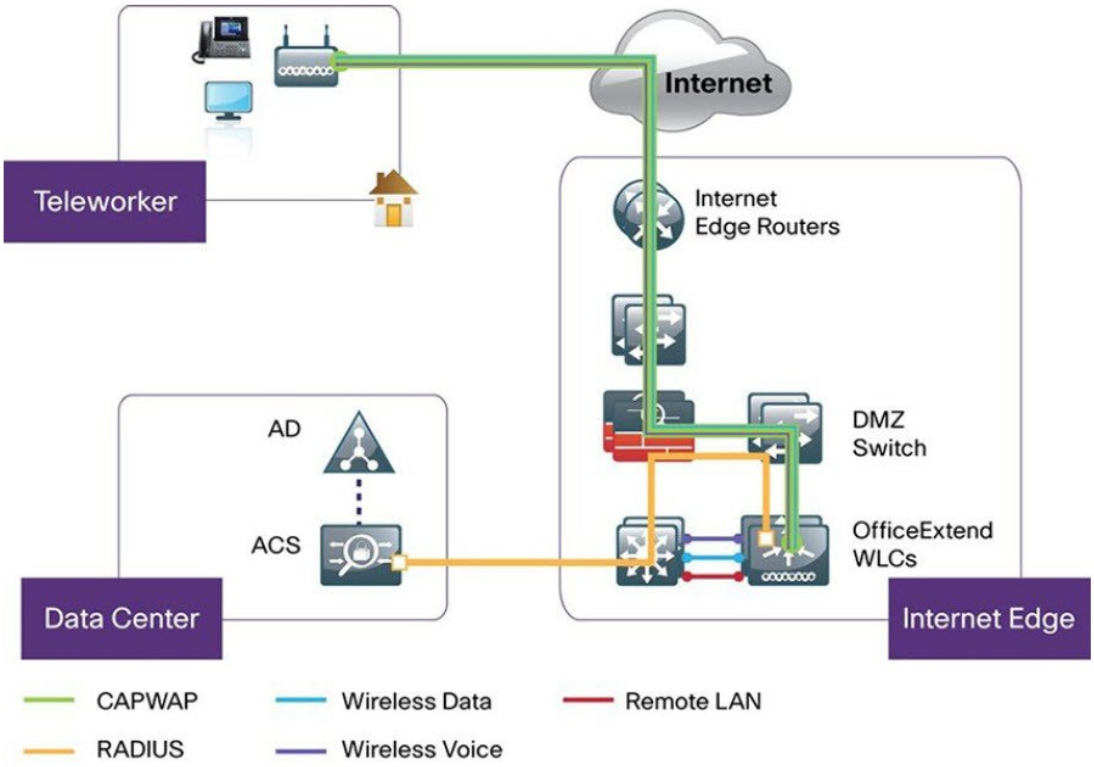
Corporate firewall

The controller should be placed in a demilitarized zone (DMZ) and the corporate firewall must allow CAPWAP control and data traffic through the firewall to the controller. The general configuration on the firewall is to allow CAPWAP control and CAPWAP management port numbers through the firewall. The UDP 5246 and 5247 ports need to be opened on the firewall for communication between the controller and the AP.

Deployment configuration

For the most flexible and secure remote teleworker configuration, deploy a dedicated controller pair in a dedicated to the Internet edge DMZ. Traffic from the Internet terminates in the DMZ versus in the internal network, while the remote AP is still directly connected to the internal network.

Figure 27: Sample remote teleworker deployment scenario



Create a remote teleworker site

A remote teleworker site is a dedicated site that is used only to manage wireless controllers and remote teleworker access points (APs). To create a remote teleworker site, you need to enable the remote teleworker function on the site. When enabled, the remote teleworker function can't be independently disabled for a site, building, or floor within the site's hierarchy. The site can only manage remote teleworker functions.

In a teleworker site, switching is performed centrally from the controller. You can't configure the network profile for FlexConnect with local switching.

Before you begin

- Understand the supported devices that are used in a teleworker deployment.
- Make sure that you have a Cisco Wireless Controller and Cisco APs in your inventory. If not, discover the devices or add them manually. For more information, see Discover Your Network, on page 55 or Add a network device, on page 130.
- Configure global wireless network settings appropriate for your network. For more information, see Configure global wireless settings, on page 350.
- For remote teleworker APs, we recommend that you create an AP profile with remote teleworker enabled and configure custom site tags. For more information, see Configure additional settings for an AP profile for Cisco IOS XE devices, on page 431 and Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475.

- For Cisco AireOS devices, you must map the AP profile to the custom AP group of the site that will be used for the remote teleworker AP. For more information, see Create network profiles for wireless, on page 460 and Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475.

Procedure

Step 1 Create a site to manage remote teleworker APs. See Create, edit, and delete a site, on page 240.

Step 2 Add buildings and floors. See Add, edit, and delete a building, on page 242.

Step 3 Configure the wireless network settings for the remote teleworker site.

a) From the main menu, choose **Design** > **Network Settings** > **Wireless**.
b) From the left hierarchy tree, select the remote teleworker site.
c) Click **Remote Teleworker**.
d) Check the **Enable Remote Teleworker** check box.
e) Click **Save**.

Step 4 Assign the controller to the site. See Assign an unprovisioned device to a site, on page 156.

Step 5 Assign the APs to the site. See Assign an unprovisioned device to a site, on page 156.

You can use serial numbers or MAC addresses but not a mixture of both, or you can upload a CSV file.

Step 6 In the wireless network settings, add the APs to the authorized APs list.

a) From the left hierarchy tree, select Global.
b) From the main menu, choose **Design** > **Network Settings** > **Wireless**.
c) Click **Security Settings**.
d) Click the **AP Authorization List** tab and add the APs that are allowed to join the controller. For more information, see Create an AP authorization list, on page 417.

The controller responds only to CAPWAP requests from APs that are in its authorization list.

Step 7 Provision the controller.

a) From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

b) Locate the controller that you want to provision.
c) Check the check box next to the device name.
d) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
e) In the **Assign Site** window, verify the assigned site, and click **Save**.
f) Click **Next**.
g) (Optional) On the **Configuration** window, under **NAT Address for Remote Teleworker**, click the **Enable NAT Address** check box and enter the NAT IP address.

Note Note that Catalyst Center does not support these addresses:

- IPv6 Documentation addresses: 2001:db8::/322
- IPv6 Site Local addresses: fec0::/103
- IPv6 Link Local addresses: fe80::/104
- IPv6 Loopback addresses: ::1
- IPv6 Multicast addresses: FF00::/8

h) Click **Next**.
i) In the **Feature Templates** window, click **Next**.
j) In the **Advanced Configuration** window, click **Next**.
k) In the **Summary** window, review the configuration settings, and click **Deploy**.
l) In the **Provision Device** slide-in pane, choose **Now**, and click **Apply**.

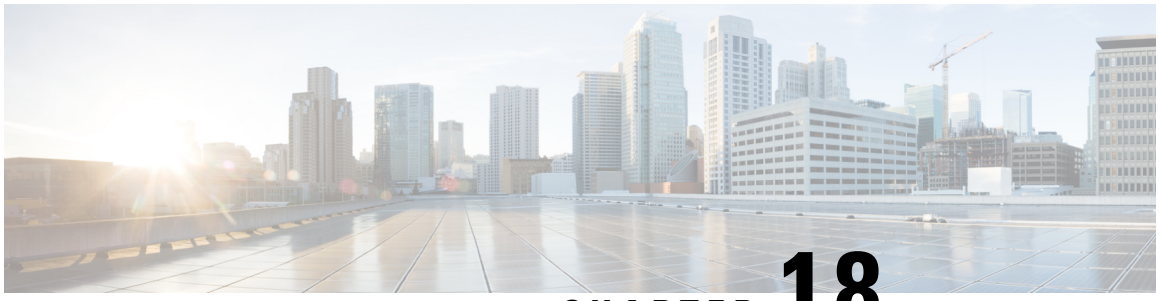
Note After deploying the configuration on the devices, the **Task Progress** bar displays the progress of the ongoing provisioning task under **Activities** > **Tasks** (which you can view by clicking the task name).

Step 8 After the Cisco Wireless Controller is provisioned, you can provision the APs.

a) From the main menu, choose **Provision** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

b) Locate the APs that you want to provision.
c) Check the check box next to the device names.
d) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.
e) In the **Assign Site** window, click **Choose a floor**, and assign the APs to a floor.
f) Click **Save**.
g) Click **Next**.
h) In the **Configuration** window, click **Next**.
i) In the **Summary** window, review the configuration settings, and click **Deploy**.
j) In the **Provision Device** slide-in pane, choose **Now**, and click **Apply**.



CHAPTER 18

Provision a Routing Profile

- Provision a router, on page 981
- VPC Inventory collection, on page 983

Provision a router

Before you begin

Make sure that you have defined the global network settings before provisioning a routing profile, including:

- Network servers, such as AAA, DHCP, and DNS. For more information, see Configure global network servers, on page 321.
- Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, Add global SNMPv3 credentials, on page 325, and Add global HTTPS credentials, on page 327.
- IP address pools. For more information, see Configure IP address pools, on page 337.
- Service provider profiles. For more information, see Configure service provider profiles, on page 350.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The **Inventory** window displays with the discovered devices listed.

Step 2 To view devices available in a particular site, click **Global** and choose the desired site, building, or floor.

All the devices available in the selected site display in the **Inventory** window.

Step 3 At the top of the **Inventory** window, click **Routers**.

Step 4 Check the check box next to the device that you want to provision.

Step 5 Click **Assign** under the site and then, in the **Assign Device to Site** window, click **Choose a site**.

Step 6 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 7 To provision a router:

a. Review the details in the **Confirm Profile** page and click **Next**.

b. Review the details in the **Router WAN Configuration** page.

   If you are provisioning a virtual router, this page is not displayed.

   1. If you chose gigabit Ethernet as the line interface, click the connection icon ○. If you choose a static IP address, enter the WAN IP address. If you choose DHCP, enter the IP address from the DHCP server. If the primary WAN is already configured using PnP, you can choose **Do not Change**. From the **Interface Name** drop-down list, choose the interface that is configured as the primary WAN.
   2. If you chose cellular as the line interface, click the connection icon ○, choose **IP Negotiated**, choose the **Interface Name** from the drop-down list, and enter the **Access Point Name (APN)**. Depending on your service provider, check the **PAP** or **CHAP** check box.
   3. Enter the **IP SLA Address** for the backup WAN interface if you have multiple service providers.
   4. Click **Next**.

c. Review the details in the **Router LAN Configuration** page.

   1. Choose the **Interface** from the drop-down list.
   2. Choose the **IP-Pool/IP** from the drop-down list.
   3. Choose the **IP Address Pool** from the drop-down list.
   4. Click **Next**.

d. Review the details in the **Integrated Switch Configuration** page.

   Depending on your configuration, this page may not be displayed.

e. Review the details in the **Summary** page by expanding the drop-down menus for the various specifications, settings, and configurations.

Step 8 Click **Deploy**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

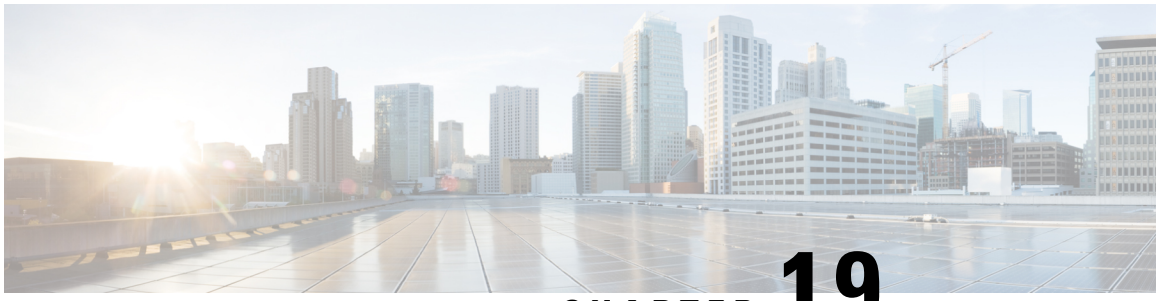
Step 10 On the **Tasks** window, monitor the task deployment.

Alternatively, you can monitor the task deployment from the **Device Inventory** window. The **Provision Status** column shows **SUCCESS** after a successful deployment. Click **SUCCESS** to see a detailed provisional log status.

VPC Inventory collection

After successful cloud inventory collection, the **Cloud** tab in the **Provision** section provides a view of the collected AWS VPC Inventory. The navigation on the left can be expanded to show the cloud regions for a cloud profile or access key. You can filter the left navigation items by keyword and click to see the VPCs just for the selected region or access key.

In the VPC Inventory view you can also click on a VPC to see more details about it, like the subnets and virtual instances in that VPC and some more details about them. AWS VPC inventory collection is scheduled to occur at the default interval for all inventory collection and can also be triggered on demand by using the **Sync** action from the gear menu for a cloud access key. The status of the inventory collection can be viewed by clicking on **Show Sync Status** in the **VPC Inventory** view.



CHAPTER 19

Provision Firewall Profiles

- Provision a firewall Threat Defense device, on page 985
- Provision a firewall Adaptive Security Appliance device, on page 987

Provision a firewall Threat Defense device

This procedure explains how to provision a Firepower Threat Defense (FTD) device managed by Firepower Management Center (FMC).

Before you begin

- Integrate FMC with Catalyst Center. See Integrate Firepower Management Center, on page 149.
- Create a site in a network hierarchy. See Create, edit, and delete a site, on page 240.
- Create a network profile for Routed FTD or Transparent FTD and assign it to a site for which the FTD device is assigned. See Create network profiles for firewall, on page 455.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the discovery process.

Step 2 Check the check box next to the FTD device that you want to provision and click **Assign** under the **Site** column.

Step 3 In the **Assign Device to Site** window, click **Choose a Site**.

Step 4 In the **Choose a Site** window, select a site from the hierarchy and click **Save**.

Step 5 Click **Next**.

Step 6 Click **Now** to assign the device to site immediately or click **Later** to schedule at a specific time.

Step 7 Click **Assign**.

Note You can view the status of assigning device to site in **Activities** > **Tasks**.

Step 8 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Provision Firewall Profile** window appears.

Step 9 Review the details in the **Confirm Profile** page and click **Next**.

Step 10 Review the details in the **Firewall Type** page and click **Next**.

The **FTD Configuration** page appears.

Step 11 If you have associated a routed mode firewall with the site, do these steps:

a) Expand the **Outside Interface** area, choose an outside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.

- **Static IP**: Enter the IP address and a subnet mask.
- **DHCP**: The IP address is obtained from DHCP.

b) Expand the **Inside Interface** area, choose an inside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.

- **Static IP**: Enter the IP address and a subnet mask.
- **DHCP**: The IP address is obtained from DHCP.

Step 12 If you have associated a transparent mode firewall with the site, do these steps:

a) Expand the **Outside Interface** area and choose an outside interface from the **Select Physical Interface** drop-down list.

b) Expand the **Inside Interface** area and choose an inside interface from the **Select Physical Interface** drop-down list.

c) Expand the **Bridge Virtual Interface** area, and do these tasks:

- **Bridge Group Number**: Enter a bridge group number. The valid number is from 1 to 250.
- **IP**: Enter the IP address of the FTD device.
- **Subnet Mask**: Enter a subnet mask.

Step 13 Click **Next**.

Step 14 In the **Summary** window, review the device specifications.

Step 15 To proceed, click **Deploy**.

The **Provision Firewall device(s)** dialog box appears.

Step 16 Click **Now**, **Later**, or **Generate configuration preview** radio button.

- **Now**: Starts the provision immediately.
- **Later**: Schedules the provisioning at a specific time.
- **Generate configuration preview**: Generates preview which can be later used to deploy on selected devices.

Step 17 Click **Apply**.

Note You can view the provisioning status in **Activities** > **Tasks**. If you chose **Generate configuration preview** in the **Provision Firewall device(s)** dialog box, you can view the work item status in **Activities** > **Tasks**.

Provision a firewall Adaptive Security Appliance device

This procedure explains how to provision a firewall Adaptive Security Appliance (ASA) device.

Before you begin

- Integrate ASA device with Catalyst Center.
- Create a network profile for the firewall for the ASA device and assign it to a site. Refer to Create network profiles for firewall, on page 455.

Procedure

Step 1 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

The Inventory page shows the device information gathered during the discovery process.

Step 2 Choose the ASA device. From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Provision Firewall Profile** window appears.

Step 3 Review the details in the **Confirm Profile** window. Click **Next**.

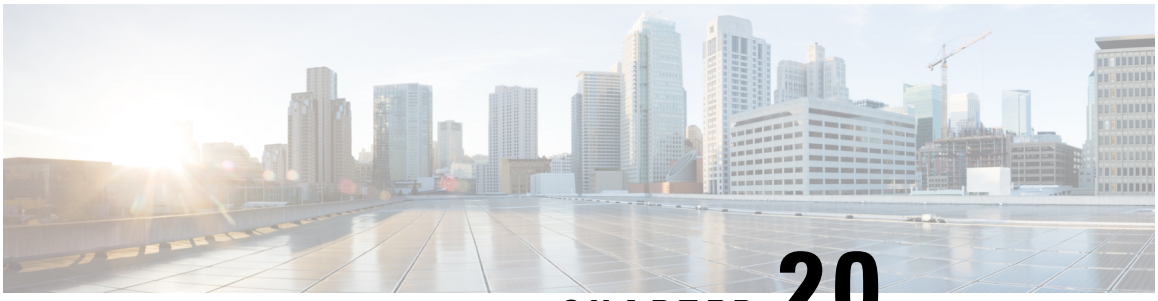
Step 4 Review the details in the **Firewall Type** window. Click **Next**.

Step 5 Review the details in the **Custom Configuration** window. Click **Next**.

Step 6 Review the device specifications in the **Summary** window. Click **Deploy**.

Depending on the Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.



CHAPTER 20

Provision a LAN Underlay

- LAN automation, on page 989
- Prerequisites for provisioning a network through LAN automation, on page 990
- Provision a network through LAN automation, on page 991
- Peer Device in LAN automation use case, on page 997
- Check the LAN automation status, on page 999
- Create a link between interfaces, on page 999
- Delete a link between interfaces, on page 1000
- Edit hostname and loopback IP address of LAN automated devices, on page 1001
- Manage devices in strict discovery mode, on page 1002

LAN automation

Catalyst Center provides LAN automation as an alternative for manual deployment of new networks. This automation allows you to simplify network operations and create a standard error-free network. LAN automation uses the IS-IS routing protocol to deploy a Layer 3 routed access design.

LAN Automation provides these capabilities:

- Provision your network through LAN automation
- View the history of LAN automation sessions
- View the summary of LAN automated devices

From the main menu, choose **Provision** > **LAN Automation** to view this window.

- **Start LAN Automation**: Use this option to initiate LAN automation sessions on your network.
- **Overview**: Expand this section to view the prerequisites and more information about provisioning your network through LAN automation.
- **Sessions**: This section consists of the **History** of LAN automation sessions, and the list of **LAN Automated Devices**.

Day-Zero Operation

On day zero, click **Start LAN Automation** to start provisioning your network through LAN automation. For more information, see Provision a network through LAN automation, on page 991.

For day zero, Catalyst Center doesn't display any data in the **Sessions** section.

Day-*n* Operation

On day *n*, you can click **Start LAN Automation** to initiate more LAN automation sessions. You can run up to five LAN automation sessions simultaneously across sites. For more information, see Provision a network through LAN automation, on page 991.

When a LAN automation session is in progress, Catalyst Center displays a tile for the session on the **LAN Automation** window. To view the details of the session, click **See Session Details** in the tile. To stop LAN automation for the session, click **Stop LAN Automation** in the tile.

The **History** tab displays the history of LAN automation sessions in your network. You can use the **Search** field to search for specific text. To view the session details, click the hyperlinked date. To view the logs for a session, in the session details window, click **View Session Logs**.

The **LAN Automated Devices** tab displays the details of the LAN automated devices. You can use the search field to filter the data based on specific text. Click one of these toggle buttons to filter the data:

- **Seed Devices**: Displays the data for seed devices
- **Discovered**: Displays the data for discovered devices
- **Provisioned**: Displays the data for provisioned devices
- **Error**: Displays the data for devices with errors

In the **LAN Automated Devices** tab, you can also do these tasks:

- Click the device name hyperlink to view the device details.
- Provision interfaces between two devices by clicking **Add Link**. For more information, see Create a link between interfaces, on page 999.
- Delete the interface between two devices by clicking **Delete Link**. For more information, see Delete a link between interfaces, on page 1000.
- Customize the hostname and loopback IP address of a device using the **Edit Device** option. For more information, see Edit hostname and loopback IP address of LAN automated devices, on page 1001.

Note

- To edit the hostname and loopback IP address of a device on Day-*n*, the device must be in the **Managed** state in the Inventory.
- You can edit the loopback IP addresses of a maximum of 25 devices in a single Day-*n* workflow.

Prerequisites for provisioning a network through LAN automation

Before provisioning a network through LAN automation, ensure these prerequisites are met:

- Configure your network hierarchy. (See Create the network hierarchy, on page 240.)
- Define these global network settings:
  - Network servers, such as the AAA, DHCP, and DNS servers. (See Configure global network servers, on page 321.)
  - Device credentials, such as the CLI, SNMP, HTTP, and HTTPS credentials. (See Add global CLI credentials, on page 323, Add global SNMPv2c credentials, on page 324, Add global SNMPv3 credentials, on page 325, and Add global HTTPS credentials, on page 327.)

Note SNMPv2 write credentials are not required and if configured, it won't be pushed to the device during LAN automation.

  - IP address pools. (See Configure IP address pools, on page 337.)
- Ensure you have at least one device in your inventory. If not, discover devices using the Discovery feature. (See Do Discovery, on page 65 and Assign an unprovisioned device to a site, on page 156.)

Note LAN automation is blocked if the discovered site is configured with "cisco" in the username of your CLI credentials.

- If you have a Cisco Catalyst 9400 Switch configured in the network, these operations must be completed on the switch for LAN automation to automatically enable the 40G port:
  - The day-zero configuration is performed on the switch.

    For more information, see “Initial Configuration for the Switch” in the *Cisco Catalyst 9400 Series Switches Hardware Installation Guide*.
  - A 40G Quad Small Form-Factor Pluggable (QSFP) transceiver is inserted in either port 9 or port 10 of the Supervisor, and the ports numbered 1 to 8 on the Supervisor do not have a 10G or 1G Small Form-Factor Pluggable (SFP) transceiver that is inserted in them. If there are dual supervisor engines, ensure that the 40G QSFP is inserted in port 9.

    For more information on the Catalyst 9400 Series Supervisor, see the “Uplink Ports” topic in the *Cisco Catalyst 9400 Series Supervisor Module Installation Note*.
- See *Cisco Catalyst Center SD-Access LAN Automation Deployment Guide* for more information on LAN automation prerequisites.

Provision a network through LAN automation

Before you begin

Make sure that the prerequisites have been met. For more information, see Prerequisites for provisioning a network through LAN automation, on page 990.

Procedure

Step 1 Reserve an IP address pool for the site that you are provisioning.

Note The size of the LAN automation IP address pool must be at least 25 bits of netmask or larger.

a) From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.
b) From the left hierarchy tree, select the required site.
c) Click the **Reserve IP Pool** link.
d) In the **Reserve IP Pool** slide-in pane, complete these fields to reserve all or part of an available global IP address pool for the selected site:

- **IP Address Pool Name**: Unique name for the reserved IP address pool.
- **Type**—Type of IP address pool:
  - **LAN**: Assigns IP addresses to LAN interfaces for applicable underlays. Choose this option for LAN automation.
  - **Management**: Assigns IP addresses to management interfaces.
  - **Service**: Assigns IP addresses to service interfaces.
  - **WAN**: Assigns IP addresses to WAN interfaces.
  - **Generic**: Used for all other network types. This is the default option.
- **IP Address Space**: Select either the **IPv4** or the **IPv6** check box to create an address pool. To create a dual-stack pool, select both the **IPv4** and **IPv6** check boxes.
- **Global IP Pool**: IPv4 address pool from which you want to reserve all or some of the IP addresses. You can enter text in the search field to filter the drop-down list's results.

Note LAN automation uses only the IPv4 subnet.

- **Prefix length / Number of IP Addresses**—Specify how to choose the IP addresses you want to reserve:

If you want to ...	Then ...
reserve the addresses with a particular IP route prefix,	1. Click the **Prefix length** radio button. 2. Choose the appropriate prefix length value from the drop-down list. 3. In the **IPv4 Subnet** field, enter the subnet address you want to use.

If you want to ...	Then ...
reserve a specific number of addresses,	1. Click the **Number of IP Addresses** radio button. 2. In the **Total host** field, enter the number of IP addresses you want to reserve.

- **Gateway**: Gateway IP address. This field is displayed only when the **Prefix length** radio button is selected.
- **Overlapping**: Specify whether you want to enable Classless Interdomain Routing (CIDR) overlapping:

If you ...	Then ...
don't want to enable the placement of IP pools in multiple parallel IPv4 and IPv6 address spaces,	ensure that the **Off** radio button is already selected, as this is the default setting.
want to enable CIDR overlapping,	1. Click the **On** radio button. 2. Specify the address space identifier that you want to use. Either click the **Create new** radio button and enter an identifier or click the **Select existing** radio button and select an identifier from the drop-down list. **Important** Take care when you enter the name for a new address space identifier. You will not be able to change the name later.

- **DHCP Server(s)**: IP address of the DHCP servers used by your Catalyst Center deployment.
- **DNS Server(s)**: IP address of the DNS servers used by your Catalyst Center deployment.

e) Click **Reserve**.

Step 2 To initiate the discovery and provisioning of the devices:

a) From the main menu, choose **Provision** > **LAN Automation**.

b) In the **LAN Automation** window, click **Start LAN Automation**.

The workflow guides you through the configuration process.

c) In the **Seed Devices** window, select the site for the seed device and configure the attributes described in the table, as required.

Attribute	Description
Primary Seed Device	Select the primary device that Catalyst Center uses as the starting point to discover and provision new devices. **Select interfaces** for the device.
Secondary Seed Device	Select the secondary seed device. **Select interfaces** for the device.

Attribute	Description
Discovery Depth	Devices are LAN automated up to the specified level under the primary seed device. The default value for Discovery Depth is 2, and the maximum value is 5.

d) In the **Sessions Attributes** window, do these steps:

1. Choose the site to which all the newly discovered devices are assigned. This site can be different from the primary and peer sites.
2. Configure the session attributes described in the table, as required.

Attribute	Description
Principal IP Address Pool	The IP address pool that is reserved for LAN automation. Choose the IP address pool from the drop-down list.
Link Overlapping IP Pool	The IP address pool that is shared with other sites and is used to configure the /31 IP addresses on point-to-point links in the underlay. • A link that overlaps IP pool can be a subpool that is inherited from a parent site or a subpool that is defined in any other site. • A link that overlaps IP pool allows you to overlap /31 IP addresses in a multisite deployment. Hosts in different sites will be able to reuse the IP addresses on the /31 links. • If you decide to define a link that overlaps IP pool, the addresses that are defined in the **Principal IP Pool** field are used for management IPs, such as loopback address, VLAN address, and so on. **Note** For an IPv6 address pool, use the **Point-to-point IPv6 Link-Local addressing** check box to configure point-to-point links.
Point-to-point IPv6 Link-Local addressing	This option is displayed when you select an IPv6 address pool. Select the check box to enable link-local addressing for point-to-point links in the underlay.
IS-IS Domain Password	Enter the IS-IS password for LAN automation. If the password already exists on the seed device, it will be reused and not overwritten. If you do not enter a password and the device does not have one, the default domain password is used. Ensure the domain passwords on both the primary and secondary seed devices match.

Attribute	Description
OSPF	When you choose the OSPF (Open Shortest Path First) routing protocol, configure these fields: • Process Id: Enter the OSPF routing process identifier. • Area Id: Specify the OSPF area identifier for the network. • Authentication key: Provide the password or key used for OSPF message authentication.
Session Timeout	Specify a timeout value for the LAN automation session. LAN automation stops automatically when the specified time limit is reached. The value is specified in minutes and the valid range is 20 through 10080.
Advertise LAN Automation Summary Route into BGP	Select this check box if you want LAN automation to advertise the principal IP pool into BGP on the primary and peer seed device. LAN automation advertises the summary route on the seed devices only if BGP is configured on them. The check box is disabled by default. It is enabled only if the primary or the peer seed device has an autonomous system (AS) number configured.
Enable Multicast	Check this check box to enable underlay native multicast. LAN automation creates a multicast tree with seed devices as RPs and discovered devices as subscribers.

Attribute	Description

Choose a File	You can either select a hostname map file from the **Choose a File** drop-down, or upload the CSV file from a storage device.
	
	User-provided names are configured for discovered devices using the chosen CSV file that contains a mapping between serial numbers and hostnames. If the discovered device is a stack, all the serial numbers of the stack are provided in the CSV file. Optionally, it can also have a customized loopback IP address for each device. The LAN automation process assigns the specified loopback IP address for the corresponding device. If the CSV file does not contain the loopback IP address information, a random IP address from the IP pool is assigned to the device.
	
	Note
	The loopback IP address for a device can be an address from any IP address pool in the same site as the device.
	
	For strict mode of device matching, the CSV file must contain the site name as well.
	
	A sample CSV file is as follows:
	
	`standalone-switch,FCW2212L0NF,10.1.1.4`
	`stack-switch,"FCW2212E00Y,FCW2212L0GV"`

Discovered Devices Hostname Prefix	Name prefix for the devices being provisioned. When Catalyst Center provisions each device, it prefixes the device with the text that you provide and adds a unique number at the end. For example, if you input "Access" as the name prefix, each consecutive device that is provisioned is named Access-1, Access-2, Access-3, and so on.
Device Matching	Select an option for device discovery: • **Relaxed**: Hostname and loopback IP is assigned to the discovered device if the device's serial number matches the uploaded device list. • **Strict**: Device discovery is restricted to the list of devices provided. You can discover a maximum of 50 devices. To add or edit devices, see Manage devices in strict discovery mode, on page 1002.

e) In the **Review** window, look through all the LAN automation session settings. To make any changes, click **Edit**.

Step 3 In the **Review** window, click **Start**.

Catalyst Center begins to discover and provision the new devices.

LAN automation configures an IP address on the seed device of VLAN 1. If this VLAN 1 IP address of the seed device is not reachable from Catalyst Center, an error message is displayed on the **LAN Automation Status** window. Hover your cursor over the **See Details** link on this window to see the error details and possible remedial actions.

Step 4 Monitor and review the progress of the devices being provisioned.

In the **LAN Automation** window, click **See Session Details** on the status pane.

You can filter the status display and see the details of the discovered devices, or the provisioned devices, or error messages. Click **View Session Logs** to display the session logs. To view device details and logs, click the device hyperlink.



Note The provisioning of new devices may take several minutes.

Step 5 Stop the LAN automation session after all the devices have been discovered and added to the inventory. Ensure that devices are reachable and in managed state.

a) In the **LAN Automation Status** window, click **Stop LAN Automation**.

When you stop LAN automation, a **Review LAN Automation Session** workflow is triggered. This workflow allows you to review the devices that are discovered during the LAN automation session and make changes before deployment.

b) In the **Review Discovered Devices** window, you can edit the loopback IP address (Management IP address) of a device.

c) Click **Validate** to verify the edited IP address.

d) If the validation succeeds, click **Apply** to deploy the LAN automation configurations.

Step 6 (Optional) You can have multiple LAN automation sessions, with up to five sessions running in parallel. Details for each session appear on separate tiles in the **LAN Automation** window.

Consider these aspects before you start simultaneous LAN automation sessions:

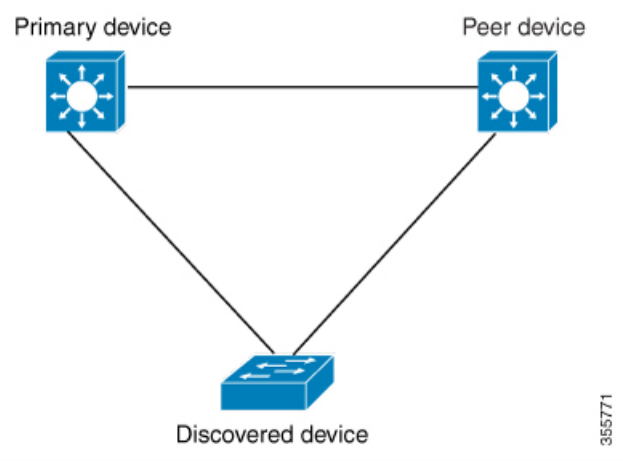
- You cannot use the same seed device for more than one session.
- You cannot use the same site for parallel sessions.
- You cannot use the same IP pool for parallel sessions.

Step 7 (Optional) You can check the status of completed LAN automation sessions under the **History** tab and see the list of discovered devices under the **LAN Automated Devices** tab.

Peer Device in LAN automation use case

Provision a dual-homed switch

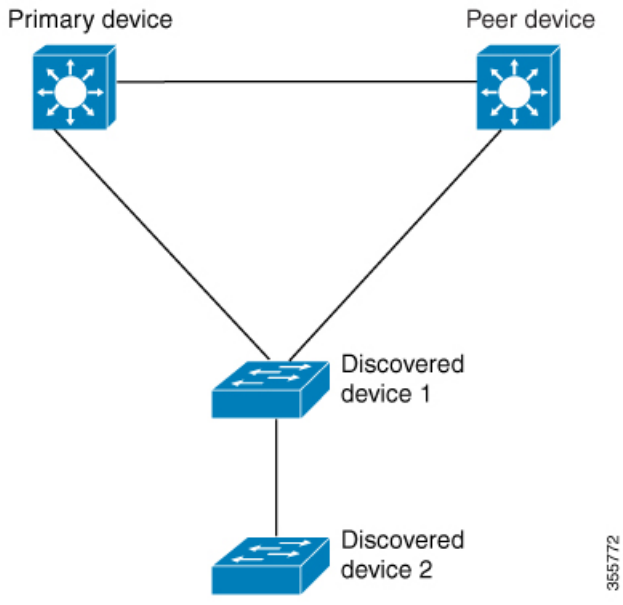
You must always select a peer device to provision the dual-homed switch.



Catalyst Center configures the DHCP server on the primary device. Because Catalyst Center understands that the discovered device is connected to both the primary and peer devices, it configures two Layer 3 point-to-point connections when the LAN automation task is stopped. One connection is established between the discovered device and the primary device; the other connection is established between the discovered device and the peer device.

Note If the link between the primary and the peer device is not configured before the LAN automation job is executed, you must select the interface of the primary device that connects to the peer device as part of the LAN automation configuration in Catalyst Center.

LAN automation two-hop limitation



For the preceding topology, Catalyst Center configures these links:

- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Primary device*
- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Peer device*
- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Discovered device 2*

Consider the scenario where a device—named *Discovered device 3*—is directly connected below *Discovered device 2*. The connection between *Discovered device 2* and *Discovered device 3* is not configured as part of the LAN automation job because it is more than two hops away from *Primary device*.

Check the LAN automation status

View the ongoing LAN automation session status and history of completed sessions, along with their logs.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

The **LAN Automation** window displays the status pane for ongoing sessions, the history of past sessions, and LAN automated devices.

Step 2 In the status pane, click **See Session Details** to view the overall status of LAN automation (In Progress or Completed) and the session logs.

Step 3 To view the history of completed sessions, select the **History** tab. Click the session hyperlink to see details and logs.

Step 4 To review LAN automated devices, select the **LAN Automated Devices** tab. Click the device name to view device-specific logs and configuration.

Create a link between interfaces

To add a link between interfaces through LAN automation:

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 On the **LAN Automation** window, in the **LAN Automated Devices** tab, click **Add Link**.

Alternatively, you can create a link from **Workflows** > **Add Link**.

Step 3 Follow these steps in the **Add Link** workflow:

a) Select the site.
b) Choose the two devices to establish the link.
c) Choose an IP address pool within the LAN.

Ensure that the IP address pool is reachable from Catalyst Center.

For IPv6, you can select the **Point-to-point IPv6 Link-Local addressing** check box to configure point-to-point links using link-local addressing.

d) Choose the interfaces on both the devices between which you want to establish a connection.
e) Click **Now** or **Later** to indicate when you want to provision the link.
f) Enter a name for the task in the field provided.
g) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
h) Click **Start Add Link**.

The **Link Configuration Started Successfully** window displays.

Step 4 (Optional) To view the status of the configuration, click **View Status in Activities**.

You can also view the status under **Activities** > **Task**.

Delete a link between interfaces

Use this procedure to delete the interface links that were created during LAN automation or by doing an Add Link operation.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 On the **LAN Automation** window, in the **LAN Automated Devices** tab, click **Delete Link**.

Alternatively, you can delete a link from **Workflows** > **Delete Link**.

Step 3 Follow the steps in the **Delete Link** workflow:

a) Select the site and two devices.
b) Select the interfaces on both these devices between which you want to delete the link.
c) Click **Now** or **Later** to indicate when you want to start the delete process.
d) Enter a name for the task in the field provided.
e) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
f) Click **Start Delete Link**.

The **LAN Automation configuration has been removed from the selected interfaces** window displays.

Step 4 (Optional) To view the status of the delete link task, click **View Status in Activities**.

You can also view the status under **Activities** > **Task**.

Edit hostname and loopback IP address of LAN automated devices

You can customize the hostname and loopback IP address of devices that are discovered through LAN automation using the reserved IP address pools of the type **LAN**.

Note

- To edit the hostname and loopback IP address of a device on Day-*n*, the device must be in the **Managed** state in the Inventory.
- You can edit the loopback IP addresses of a maximum of 25 devices in a single Day-*n* workflow.

Before you begin

- Discover the devices through LAN automation. For more information, see Provision a network through LAN automation, on page 991.
- Reserve the required IP address pools of the type **LAN**. For more information, see Reserve an IP address pool, on page 339.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 In the **LAN Automated Devices** tab of the **LAN Automation** window, check the check box next to the devices that you want to edit.

Step 3 Click **Edit Device**.

Step 4 In the **Edit Devices** window, do these steps:

a) In the **Device Name** field, enter the hostname for the device.

b) From the **IP Address Pool** drop-down list, choose an IP address pool.

c) In the **IP Address** field, enter an IPv4 address without a subnet mask.

Note The IP address must be within the range of the selected IP address pool.

d) Use the **Reset** or **Reset All** option to revert the changes, if required.

e) Repeat Step 4.a, on page 1001, Step 4.b, on page 1001, and Step 4.c, on page 1001 for each device.

f) Click **Validate**.

If the specified IP address isn't available for allocation, Catalyst Center displays an error message. Enter a valid IPv4 address in the corresponding **IP Address** field.

g) Click **Next**.

Step 5 In the **Schedule Edit Device Deployment** window, do one of these tasks:

- Click the **Now** radio button, name the task, and click **Apply**.
- Click the **Later** radio button; name the task; specify the start date, start time, and time zone; and click **Apply**.

Manage devices in strict discovery mode

With Catalyst Center Release 2.3.7.5 and later, you can choose either **Relaxed** mode or **Strict** mode for device matching during discovery. **Strict** mode limits device discovery to a defined list. Follow these steps to add, edit, or delete devices in the discovery list.

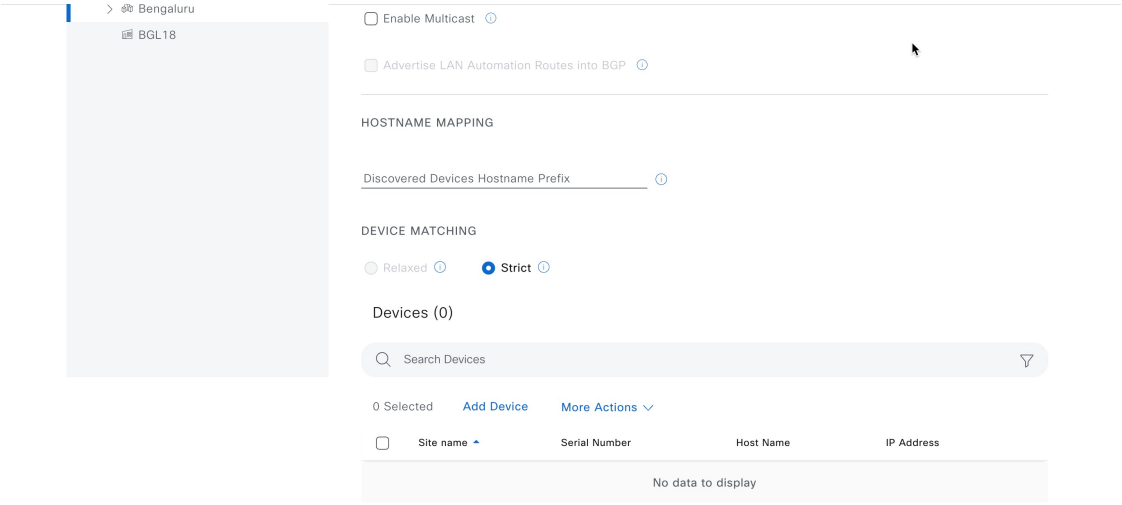
Procedure

Step 1 In the **LAN Automation** window, click **Start LAN Automation**.

Step 2 Add the seed devices and click **Next**.

Step 3 In the **Session Attributes** window, in the left pane, select a building or a floor.

Step 4 Under **Device Matching**, select the **Strict** option.



Note If you select an area as the site, you must add a device list. In this case, the **Strict** mode is chosen automatically, and the **Relaxed** mode is disabled.

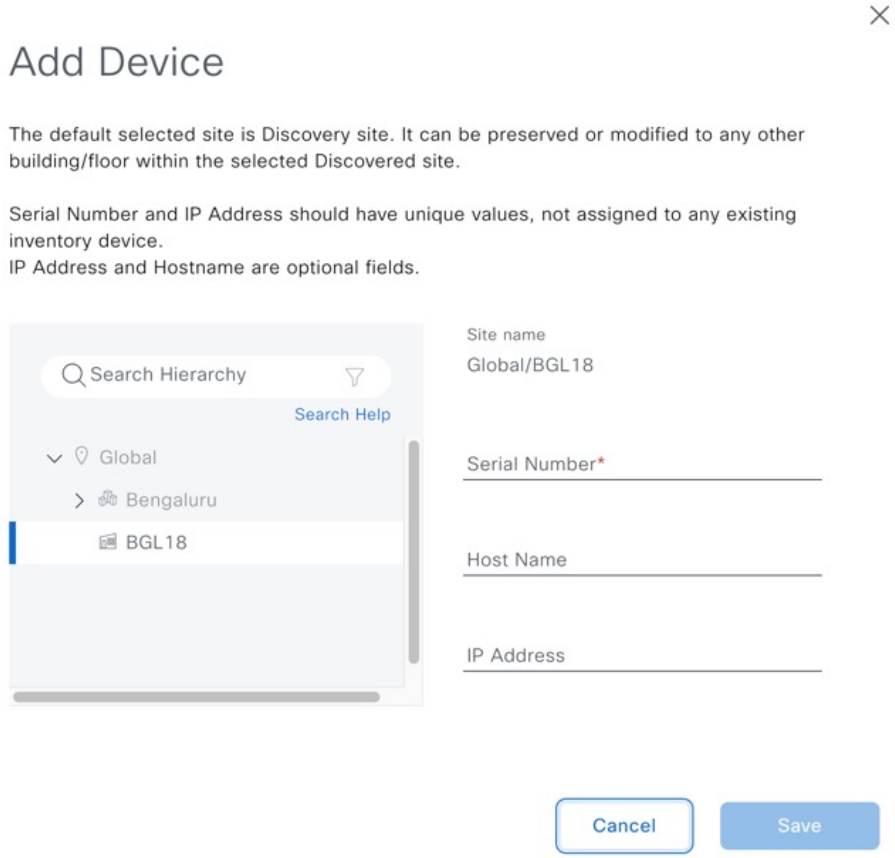
Step 5 Add devices using one of these options for your discovery list:

- **Add Device**: Use this option to add a single device.
  - In the **Devices** table, click **Add Device** and follow these steps:
    a. If you've chosen an area, select a building or a floor as the site.

b. Enter a **Serial Number** for the device.

c. (Optional) Enter the **Host Name** and **IP Address** for your device.

d. Click **Save**.



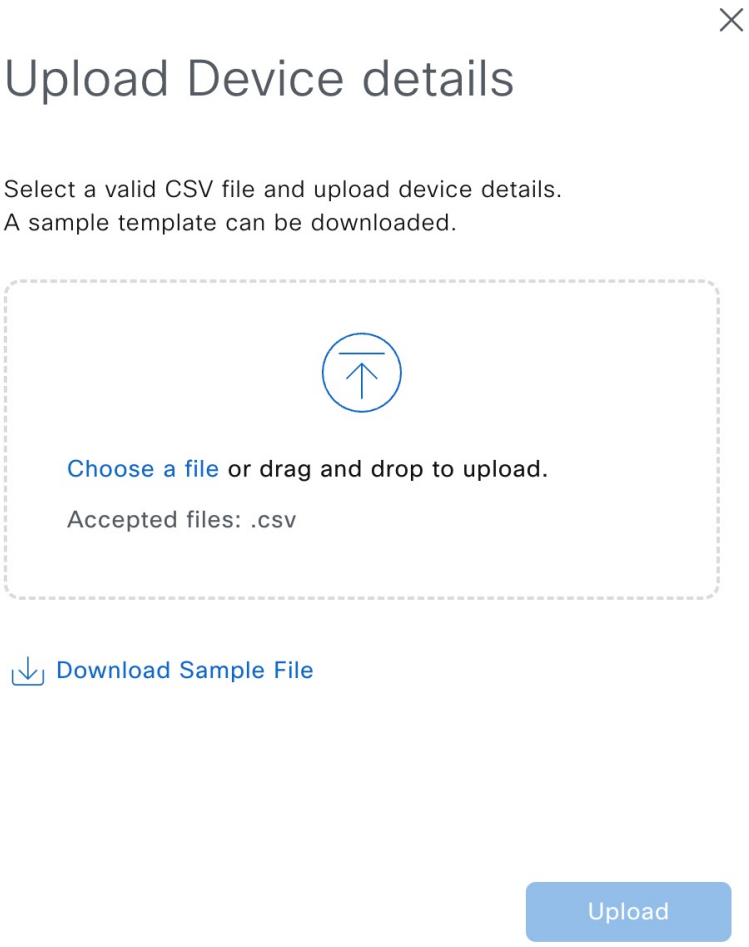
- **Upload Device**: Use this option to add devices from a CSV file.

  a. In the **Devices** table, click **More Actions** and choose the option to upload the device CSV file.

  b. Upload the CSV file.

  Drag and drop the CSV file into the boxed area or click **Choose a file** and browse to the CSV file.

  You can also download a sample template.



Step 6 Follow these steps to edit a device from the discovery list:

a) Check the check box next to the device that you want to edit and choose **More Actions** > **Edit Device**.

b) Edit the device details as needed

You can edit only one device at a time.

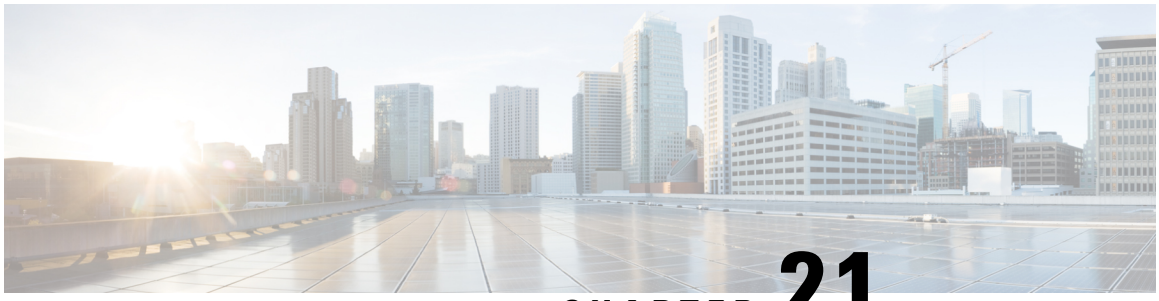
c) Click **Save**.

Step 7 Follow these steps to delete a device from the discovery list:

a) Check the check box next to the device that you want to delete and choose **More Actions** > **Delete Device**.

You can select multiple devices to delete.

b) Click the **Delete** icon and confirm the delete action.



CHAPTER 21

Provision SD-Access LISP Fabric Network

- Cisco SD-Access zero-trust security solution, on page 1005
- About fabric networks, on page 1012
- Role-based access control for Cisco SD-Access, on page 1017
- Add a fabric site, on page 1018
- Move a fabric site, on page 1020
- Configure a fabric site, on page 1021
- Add a device to a fabric, on page 1022
- Remove a device from a fabric, on page 1025
- Add a device as a border node, on page 1027
- Configure LISP Pub/Sub, on page 1030
- Reconfigure a fabric, on page 1031
- Create an IP transit, on page 1032
- Create an SD-Access transit, on page 1033
- Configure an authentication template for the fabric site, on page 1035
- Configure ports within the fabric site, on page 1036
- Configure wireless SSIDs for fabric networks, on page 1038
- Configure a wireless mesh access point in a fabric, on page 1039
- Configure security service insertion on a fabric site, on page 1039
- Virtual networks, on page 1040
- Configure a fabric zone, on page 1052
- Configure an extended node device, on page 1058
- Configure supplicant-based extended nodes, on page 1068
- Configure a port channel, on page 1074
- Multicast, on page 1077
- Edit BGP AS number for a fabric site, on page 1079
- Shared wireless controllers for multiple fabric sites, on page 1080

Cisco SD-Access zero-trust security solution

Networks need protection against external and internal threats. Cisco SD-Access provides a zero-trust security solution for your workplace. The Cisco SD-Access zero-trust security solution provides secure access to users and devices from all locations across the network.

The Cisco SD-Access zero-trust security solution includes these capabilities:

- Identify and verify all endpoints: SD-Access establishes an initial level of trust with each connecting endpoint.
- Establish policy and segmentation: SD-Access ensures least-privilege access based on the endpoint and user type.
- Continuously monitor endpoints: SD-Access continuously monitors the endpoints to ensure compliance.
- Threat mitigation: SD-Access allows you to quarantine the endpoints that are noncompliant or exhibit malicious behavior.

The Cisco SD-Access zero-trust security solution provides the flexibility to adopt a path to a zero-trust workplace based on your network settings and services. You can configure how users connect to the network using dynamic rules and automated segmentation.

The Cisco SD-Access zero-trust security solution provides the capability to automate network access policies using these features:

- Endpoint visibility: You can identify and group endpoints. You can map their interactions through traffic flow analysis and define access policies.
- Trust monitoring: You can continuously monitor the endpoint behavior, scan for vulnerabilities, verify trustworthiness for continued access, and isolate rogue or compromised endpoints.
- Network Segmentation: You can enforce group-based access policies and secure network through multilevel segmentation.

The Cisco SD-Access zero-trust security solution enables you to explore various paths to zero-trust workplace based on your network settings and services. You can discover your optimal path based on your current network status, and explore the benefits of each added step on the zero-trust journey.

Zero-Trust Overview dashboard

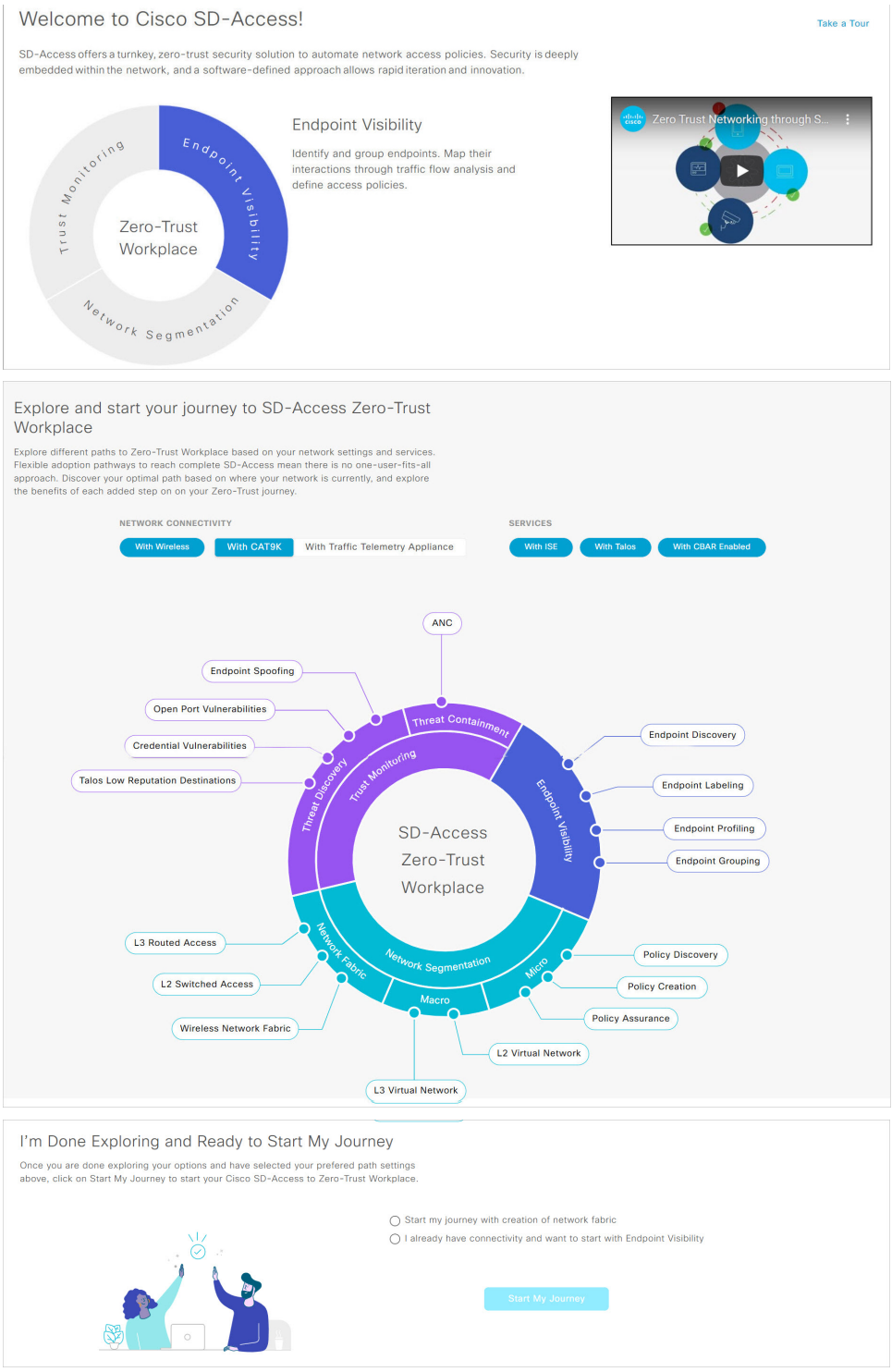
The SD-Access **Zero-Trust Overview** dashboard provides an overview of your zero-trust workplace journey. From the main menu, choose **Provision** > **Zero-Trust Overview** to view this dashboard.

The zero-trust workplace journey has these phases:

- Day zero: For starting your zero-trust workplace journey. For more information, see Day-zero view of the Zero-Trust Overview dashboard, on page 1006.
- Day *n*: For ongoing monitoring and configuration changes of your zero-trust workplace journey. For more information, see Day-n view of Zero-Trust Overview dashboard, on page 1009.

Day-zero view of the Zero-Trust Overview dashboard

Before you start your SD-Access zero-trust workplace journey, the day-zero view of the **Zero-Trust Overview** dashboard consists of these sections:



- **Welcome to Cisco SD-Access!**: This section consists of an overview video that provides a short overview of the multiple paths towards a full SD-Access zero-trust workplace. It also consists of a circle containing sections for each pillar of the SD-Access zero-trust workplace:
    - **Endpoint Visibility**

- **Trust Monitoring**
- **Network Segmentation**

Hover your cursor over each section to view more information.

- **Explore and start your journey to SD-Access Zero-Trust Workplace**: This section allows you to explore the different paths to a zero-trust workplace based on your network settings and services, and discover the optimal path for your network. This section consists of the **Network Connectivity** and **Services** options, and a circular journey map with details about the paths. Based on the options that you choose for network connectivity and services, the journey map displays the available paths to your zero-trust workplace journey.

  To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

- **I'm Done Exploring and Ready to Start My Journey**: After exploring the paths and selecting your preferred settings, use this section to start your journey to a zero-trust workplace.

Get started with SD-Access zero-trust workplace journey

Procedure

Step 1 From the main menu, choose **Provision** > **Zero-Trust Overview**.

Step 2 Under **Explore and start your journey to SD-Access Zero-Trust Workplace**, do these steps:

a) For **Network Connectivity** settings, choose the required options:

- Enable **With Wireless** to use wireless devices in your zero-trust workplace journey.
- Enable **With CAT9K** to use Cisco Catalyst 9000 Series devices or enable **With Traffic Telemetry Appliance** to use the Catalyst Center Traffic Telemetry Appliance in your zero-trust workplace journey.

b) For **Services** settings, choose the required options:

- Enable **With ISE** to use Cisco Identity Services Engine in your zero-trust workplace journey.
- Enable **With Talos** to use Talos Intelligence in your zero-trust workplace journey.
- Enable **With CBAR Enabled** to use Controller-Based Application Recognition (CBAR) in your zero-trust workplace journey.

c) (Optional) To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

Step 3 Under **I'm Done Exploring and Ready to Start My Journey**, choose one of these options:

- To create a fabric network and start your journey towards a zero-trust workplace, click **Start my journey with creation of network fabric**.
- If you already have fabric network connectivity and want to start your journey towards zero-trust workplace with endpoint visibility, click **I already have connectivity and want to start with Endpoint Visibility**.

Step 4 Click **Start My Journey**.

Step 5 In the **Modify Journey Map** dialog box, do these steps:

a) Review your journey map settings.

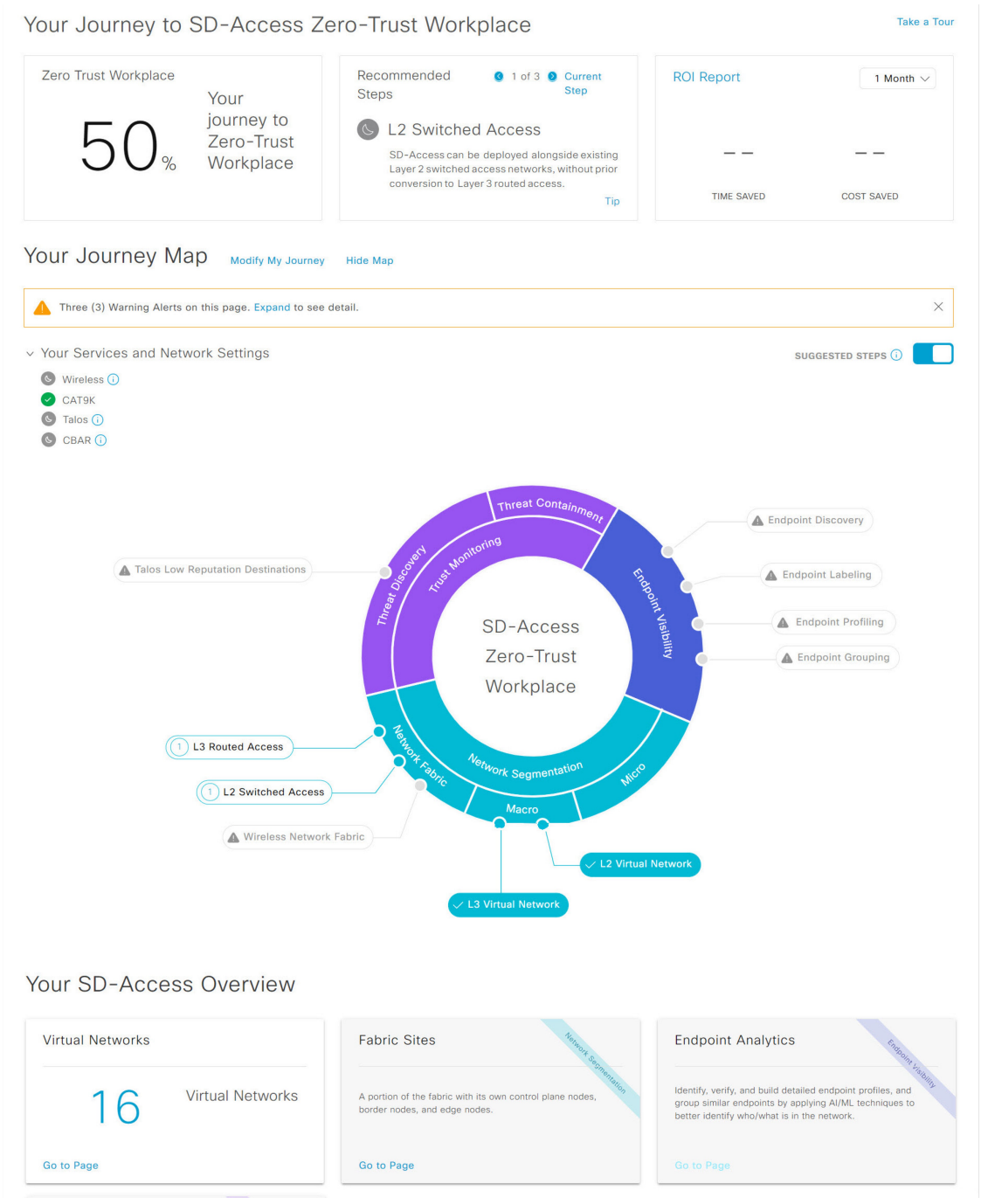
Note
- Catalyst Center displays a message if it doesn't discover the selected services for your network.
- Catalyst Center displays a message if it discovers additional services that were not selected in the journey.

b) (Optional) To remove a selected service from your journey map settings, uncheck the corresponding check box.

c) Click **Confirm**.

Day-*n* view of Zero-Trust Overview dashboard

After starting your SD-Access zero-trust workplace journey, the day-*n* view of the **Zero-Trust Overview** dashboard consists of these sections:



- **Your Journey to SD-Access Zero-Trust Workplace**: This section consists of these dashlets:
  - The **Zero Trust Workplace** dashlet displays the percentage progress of your zero-trust workplace journey.
  - The **Recommended Steps** dashlet displays the next recommended steps for your zero-trust workplace journey. Use the arrow buttons (and) to scroll through all the steps. This dashlet also displays the tips for some steps. If available, click **Tip** to view the tips for the corresponding step.

- The **ROI Report** dashlet displays the time and cost savings based on the implemented steps as you progress through your zero-trust workplace journey. Use the drop-down in this dashlet to choose the time period for the report. Click **ROI Report** to view the report.

- **Your Journey Map**: This section displays the details of network connectivity and service settings for your zero-trust workplace journey. Click **Modify My Journey** to modify your zero-trust workplace journey. Click **Hide Map** to hide the journey map.

  This section displays the warning alerts for your journey, if available. Click **Expand** to view the details of the alerts. If a selected service is currently unavailable in your network and you want to remove it from your journey, click the corresponding **Remove From Journey** option. If you want to get a selected service that is currently unavailable in your network, click the corresponding hyperlink to get the service.

  Expand the **Your Services and Network Settings** drop-down to view the list of selected services for your journey. The icon next to a service indicates that the service is currently available in your network. The icon next to a service indicates that the service is currently unavailable in your network. Hover your cursor over the corresponding icon to view the **Update Needed** dialog box with details about the unavailable service. In the **Update Needed** dialog box, do these tasks:

  - To remove the service from your journey, click **Remove From Journey**.
  - To get the unavailable service in your network, click the corresponding hyperlink.

  Enable the **Suggested Steps** toggle button to view the suggested order of steps around your journey map.

  To view details about each step in the journey map, hover your cursor over the corresponding step around the journey map.

  The icon next to a step indicates that the corresponding configurations are incomplete. A number next to a step (for example, 1) indicates the suggested order of the recommended steps for your journey map. The icon next to a step indicates that the corresponding configurations are complete.

- **Your SD-Access Overview**: This section consists of dashlets for each functional area of your zero-trust workplace journey. Click the corresponding **Go to Page** option to open the relevant window. Each dashlet indicates its corresponding pillar of the zero-trust workplace journey in its upper-right corner.

Modify SD-Access zero-trust workplace journey

Procedure

Step 1 From the main menu, choose **Provision** > **Zero-Trust Overview**.

Step 2 Under **Your Journey Map**, click **Modify My Journey**.

Step 3 Under **Explore and start your journey to SD-Access Zero-Trust Workplace**, do these steps:

a) For **Network Connectivity** settings, choose the required options:

- Enable **With Wireless** to use wireless devices in your zero-trust workplace journey.
- Enable **With CAT9K** to use Cisco Catalyst 9000 Series devices or enable **With Traffic Telemetry Appliance** to use the Catalyst Center Traffic Telemetry Appliance in your zero-trust workplace journey.

b) For **Services** settings, choose the required options:

- Enable **With ISE** to use Cisco Identity Services Engine in your zero-trust workplace journey.
- Enable **With Talos** to use Talos Intelligence in your zero-trust workplace journey.
- Enable **With CBAR Enabled** to use Controller-Based Application Recognition (CBAR) in your zero-trust workplace journey.

c) (Optional) To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

Step 4 Under **I'm Done Exploring and Ready to Start My Journey**, choose one of these options:

- To create a fabric network and start your journey towards a zero-trust workplace, click **Start my journey with creation of network fabric**.
- If you already have fabric network connectivity and want to start your journey towards zero-trust workplace with endpoint visibility, click **I already have connectivity and want to start with Endpoint Visibility**.

Step 5 Click **Modify My Journey**.

Step 6 In the **Modify Journey Map** dialog box, do these steps:

a) Review your journey map settings.

Note

- Catalyst Center displays a message if it doesn't discover the selected services for your network.
- Catalyst Center displays a message if it discovers additional services that were not selected in the journey.

b) (Optional) To remove a selected service from your journey map settings, uncheck the corresponding check box.

c) Click **Confirm**.

About fabric networks

A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

Catalyst Center allows you to add devices to a fabric network. These devices can be configured to act as control plane, border, or edge devices within the fabric network.

Fabric sites

A fabric site is an independent fabric area with a unique set of network devices: control plane, border, edge, wireless controller, ISE PSN. Different levels of redundancy and scale can be designed per site by including local resources: DHCP, AAA, DNS, Internet, and so on.

A fabric site can cover a single physical location, multiple locations, or only a subset of a location:

- Single location: branch, campus, or metro campus
- Multiple locations: metro campus + multiple branches
- Subset of a location: building or area within a campus

A Software-Defined Access fabric network may comprise multiple sites. Each site has the benefits of scale, resiliency, survivability, and mobility. The overall aggregation of fabric sites accommodates a large number of endpoints and scales modularly or horizontally. Multiple fabric sites are interconnected using a transit.

Transits

A transit is a site that interconnects two or more fabric sites or connects the fabric site with external networks (Internet, data center, and so on). There are two types of transit networks:

- IP transit: Uses a regular IP network to connect to an external network or to connect two or more fabric sites. It leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.
- SD-Access transit: Uses LISP/VxLAN encapsulation to connect two fabric sites. The SD-Access transit area may be defined as a portion of the fabric that has its own control plane nodes, but does not have edge or border nodes. However, it can work with a fabric that has an external border. With an SD-Access transit, an end-to-end policy plane is maintained using SGT group tags.

Fabric readiness, image compatibility, and compliance checks

Fabric readiness checks

Fabric readiness checks are a set of preprovisioning checks done on a device to ensure that the device is ready to be added to the fabric. Fabric readiness checks are now done automatically when the device is provisioned. Interface VLAN and Multi VRF configuration checks are not done as part of fabric readiness checks.

Fabric readiness checks include:

- Connectivity check: Checks for the necessary connectivity between devices; for example, connectivity from the edge node to map server, from edge node to border, and so on.
- Existing configuration check: Checks for any configuration on the device that conflicts with the configuration that is pushed through SD-Access and can result in a failure later.
- Hardware version: Checks if the hardware version of the device is supported.
- Image type: Checks if the device is running with a supported image type (IOS-XE, IOS, NXOS, Cisco Controller).
- Loopback interface: Checks for the loopback interface configuration on the device. A device must have a loopback interface numbered 0 with an IP address configured on it to work with the SDA application. Lack of a loopback interface numbered 0 may cause fabric provisioning errors because Loopback0 is used as the routing locator (RLOC) by default.
- Software license: Checks if the device is running with an appropriate software license.

If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. You can correct the problem and continue with the provisioning workflow for the device.

Image compatibility check

To ensure the network devices (before and after a fabric deployment) are compatible with the recommended or supported software image versions based on the Catalyst Center package version, Catalyst Center performs Image Compatibility check to evaluate the network devices.

If a network device is running an incompatible software image, the  icon is displayed in the **Provision** > **Inventory** > **Image Compatibility** column. You can check the supported software image versions for your device from the *Cisco SD-Access Compatibility Matrix* and continue with the provisioning workflow for the device.

Fabric compliance checks

Fabric compliance is a state of a device to operate according to the user intent configured during the fabric provisioning. Fabric compliance checks are triggered based on:

- Every 24 hours for wired devices and every six hours for wireless devices.
- When there is a configuration change on the wired device.

  A configuration change on the wired device triggers an SNMP trap, which in turn triggers the compliance check. Ensure that you have configured the Catalyst Center server as an SNMP server.

These compliance checks are done to ensure that the device is fabric compliant:

- Virtual Network: Checks whether the necessary VRFs are configured on the device to comply with the current state of the user intent for the VN on Catalyst Center.
- Fabric Role: Checks whether the configuration on the device is compliant with the user intent for a fabric role on Catalyst Center.
- Segment: Checks the VLAN and SVI configuration for segments.
- Port Assignment: Checks the interface configuration for the VLAN and authentication profile.

Fabric Health Check

The health of SD-Access application is checked periodically to provide an indication of the application status. SD-Access health check also includes the check for stale database entries in the SD-Access application, which could potentially disrupt fabric provisioning.

You can check the status of SD-Access application on the **System** > **System 360** > **System Health** page. For more information about how to check the health of an application, see “Use System 360” and “Monitor System Health” in the Cisco Catalyst Center Administrator Guide.

You can also use the Validation Tool to run the same checks by subscribing to the SD-Access Application Health status. Validation Tool is available on the **System** > **System 360** > **System Health** page. When you run a new validation, ensure that you check the **Application Health Status** check box under the **Validation Set(s) selection** field. For more information on how to access and run the Validation Tool, see “Use the Validation Tool” in the Cisco Catalyst Center Administrator Guide.

SD-Access application status can have three values:

- **HEALTHY**—Indicates that the SD-Access application is working as expected and all provisioning activities are allowed.
- **UNHEALTHY**—Indicates that the SD-Access application is not working due to dependent services not being healthy. This condition may block all provisioning activities in the SD-Access fabric.
- **DEGRADED**—Indicates that all dependent services are working but there are database inconsistencies in the SD-Access application. This condition may affect the functioning or provisioning of one or more fabric sites.

  If your SD-Access application is in the DEGRADED state, contact Cisco TAC to resolve the issue.

Fabric scale checks

Scale checks monitor the scale limits or thresholds defined for entities in a fabric site. It provides visibility into the number of fabric entities that are approaching or exceeding the defined scale limits. Scale checks are performed whenever an entity is provisioned in the fabric site.



Note Scale checks serve as a guideline to provide visibility for potential scale violations and do not impose any enforcement that would prevent the provisioning of additional fabric entities.

You can view the scale check status under the **Application Checks** column in the **Provision** > **SD-Access** > **Fabric Sites** window. The **Application Checks** column displays these states based on the scale check results:

- Critical: Indicates that a fabric entity has exceeded 95% of its defined scale limits.
- Warning: Indicates that a fabric entity has crossed 75% of its defined scale limits.
- Green check mark: Indicates that there are no issues with the SD-Access application.
- Not Applicable: Indicates that there are no entities associated with the fabric site.

For Critical and Warning status, you can click the indicator to view more information on the scale checks.

For information on scale thresholds per fabric site, see "Appliance scale" in *Cisco Catalyst Center Data Sheet*.

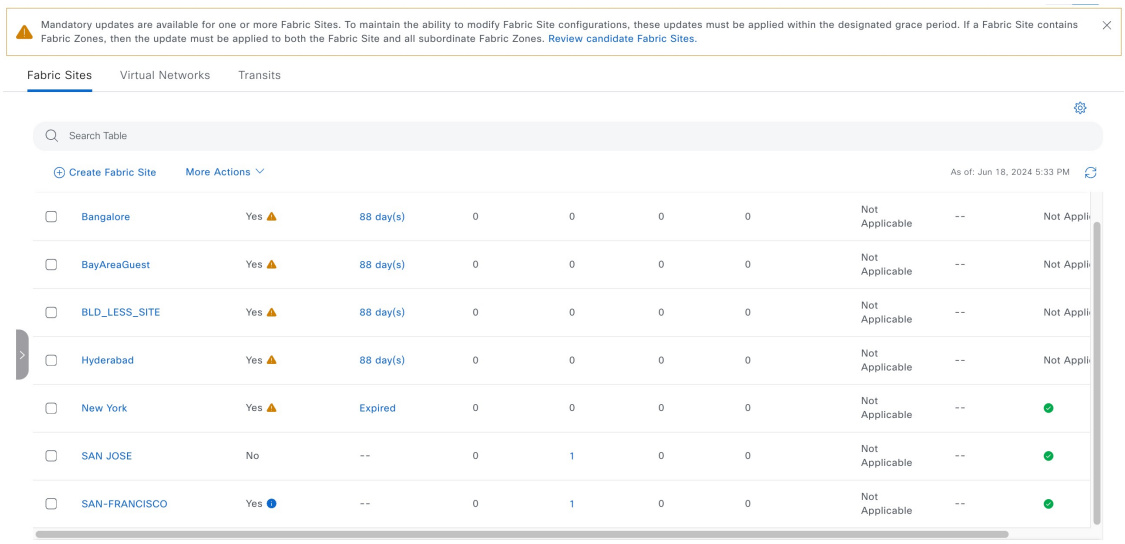
Fabric site updates

The **Fabric Sites** overview page provides information on the configuration updates available for the fabric sites and the grace period to apply these updates. It displays a banner message to apply the mandatory configuration updates available for the sites within a designated grace period. If the grace period expires (by default, 180 days), no configurations on the fabric site can be done until the updates are applied. You can click the **Review candidate Fabric Sites** link in the banner to view the fabric sites that need mandatory updates.

Columns in the **Fabric Sites** table display the configuration update information, including:

- **Outstanding Updates**: Displays **Yes** or **No** based on the updates available for the site and its associated zones.

- **Update Grace Period**: Displays the least time left (number of days) among the fabric site and its associated zones to apply the updates. You can click the value to view the individual grace period for the site and its associated zones.





This table describes the values displayed in these columns.

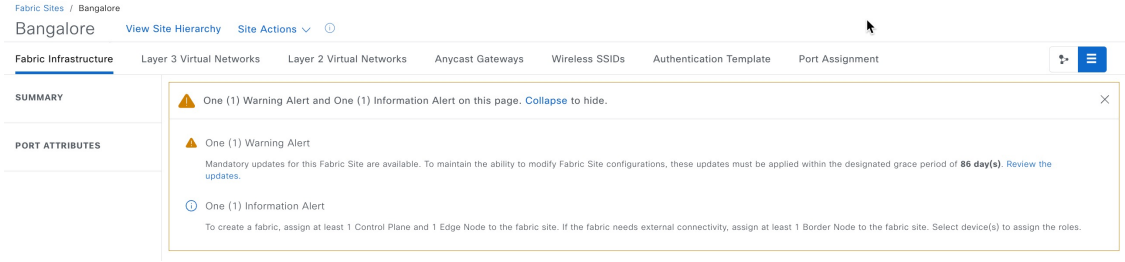
Outstanding updates	Update grace period	Description
Yes with an info icon.	Displays a blank value.	Indicates that the updates are available but the prerequisites have not been met and hence there is no timer for applying the updates. The grace period timer starts once the prerequisites are met and the updates are ready to be applied.

Outstanding updates	Update grace period	Description
Yes with a warning icon.	Displays the least time left (number of days) among the fabric site and its associated zones to apply the updates. If the grace period has expired for a site or any of its associated zones, the column displays **Expired**.	Indicates that the site or its associated zones have outstanding updates. Click the value to view the individual grace period for the site and its associated zones.
No	Displays a blank value.	Indicates that there are no outstanding updates for the site and its associated zones.

When you click on a site with an outstanding update, the fabric site window displays alerts for the configuration update based on the availability of updates and the grace period, as follows:

- Ready updates with active grace period: Displays a warning pop-up window and an alert about the availability of updates and the grace period to apply the updates.
- Ready updates with expired grace period: Displays an error pop-up window and a critical alert that the grace period for the updates has expired and all fabric site configurations are suspended.
- Not ready updates: Displays an information alert that the updates for the site are available but the prerequisites have not been met. You can review the available updates and prepare for implementation.

In the alert dialog box, click **Expand** to view the alert details and click the **Review the updates** link to view and apply the available updates.



Role-based access control for Cisco SD-Access

Role-based access control in Catalyst Center allows you to create custom roles, which define the capabilities and the permissions that a user has access to. For Cisco SD-Access, Catalyst Center supports the creation of a custom role with the **SD-Access** capability that

- simplifies the role-based access control configuration for Cisco SD-Access fabric.
- allows users assigned with the custom role to create and manage an SD-Access fabric, and
- avoids manual configuration of access permissions for dependent functionalities. When you set the access permissions for **SD-Access**, all the other dependent capabilities such as device discovery, device provision, PnP, compliance, and SWIM are automatically selected with the necessary permissions. It is recommended not to reconfigure these permissions manually.

For more information on configuring custom roles in Catalyst Center, see *Cisco Catalyst Center Administrator Guide*.

Add a fabric site

Before you begin

You can create a fabric site only if IP Device Tracking (IPDT) is already configured for the site. To enable IPDT, go to **Design** > **Network Settings** > **Telemetry** and in the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button.

Ensure these requirements are met for IPv6 underlay support.

- Supported platforms: Cisco IOS XE 26.1.1 and later, Cisco ISE Release 3.5 Patch 3.
- Supported products: Cisco Catalyst 9000 Series Switches.

  Cisco Catalyst 9200, IE9300, and IE3500 Series Switches are not supported in fabric edge roles but are supported in extended node and policy extended node roles. Cisco Catalyst 9200 Series Switches are supported in supplicant based extended role.

  Cisco Catalyst C9350, C9610, 9550, 9600x, and 9500x Series Switches are not supported for any fabric roles in an IPv6 underlay fabric and for dual stack border role in an IPv4 fabric site.
- A fabric site supports either IPv4 or IPv6 underlay, but not both.
- IPv6 underlay is supported only with LISP Pub/Sub SDA fabric.
- IPv6 overlay multicast is supported in HER/Unicast mode for both IPv4 and IPv6 underlay fabric sites.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of the fabric sites.

The resulting window displays every fabric site that has already been created and its information (such as Health Score, Fabric Zones, Fabric Devices, Fabric Roles, and Connected Transits) in a tabular format.

You can customize the table view to display only selected columns. Use the gear icon at the top right corner of the window to edit the **Table Settings** and **Apply** the changes.

Step 3 Click **Create Fabric Sites**.

Alternatively, instead of the first three steps, click the menu icon and choose **Workflow** > **Create Fabric Sites and Fabric Zones**.

Step 4 In the **Create Fabric Sites** window, click **Let's Do it** to go directly to the workflow.

Step 5 In the **Fabric Site Location** window, select an area, building, or floor to add as a fabric site.

Step 6 In the **Wired Endpoint Data Collection** window, ensure that the **Wired Endpoint Data Collection** check box is checked.

Step 7 Choose the **Underlay IP Addressing** for the fabric.

- For dual stack Catalyst Center deployments, you can choose either **IPv4** or **IPv6**.
- For single stack Catalyst Center deployments, the underlay IP addressing type is chosen by default, either **IPv4** or **IPv6**.

Step 8 In the **Authentication Template** window, do these steps:

a) Select an authentication template for the fabric site:

Template option	Description
Closed Authentication	Any traffic before authentication is dropped, including DHCP, DNS, and ARP.
Open Authentication	A host is allowed network access without having to go through 802.1X authentication.
Low Impact	Security is added by applying an ACL to the switch port, to allow very limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.
None	None.

b) (Optional) If you select **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:

Setting	Task
First Authentication Method	Select **802.1x** or **MAC Authentication Bypass (MAB)**.
802.1x Timeout (in seconds)	Use the slider to specify the 802.1x timeout, in seconds.
Wake on LAN	Select **Yes** or **No**.
Number of Hosts	Select **Unlimited** or **Single**.
Voice VLAN	Use this check box to enable or disable the default voice VLAN (VLAN 2046) for the site.
BPDU Guard	Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
Pre-Authentication Access Control List	You can configure Pre-authentication Access Control List (ACLs) for IPv4 and IPv6. **1.** Enable the toggle button to configure preauthentication control for **Low Impact** authentication. **2.** From the **Implicit Action** drop-down list, choose an implicit action and enter a description for the rule. **3.** To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

Step 9 (Optional) In the **Fabric Zones** window, choose one of these options:

Option	Task
To designate fabric zones later	Click **Setup Fabric Zones Later**.
To designate fabric zones and create scoped subnets	Click **Setup Fabric Zones Now** and select a fabric site from the displayed network hierarchy.

Step 10 In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

Step 13 It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a Fabric Site Creation Completed message displays.

Next, you are provided with options to either create a new fabric site or view the activities on the **Tasks** window.

Move a fabric site

After creating a fabric site, you can change the site hierarchy in these ways:

- A fabric site can't be moved under another fabric site; nesting of fabric sites isn't permitted.
- Once a site, building, or floor is part of a fabric site (either as a fabric zone or as a member in the fabric site), it must remain within that fabric site's hierarchy. It can't be moved outside of it.
- To prevent conflicts during a move, the system verifies that network settings and network profiles match between the current and new parent sites.

Figure 28: Sample site hierarchy

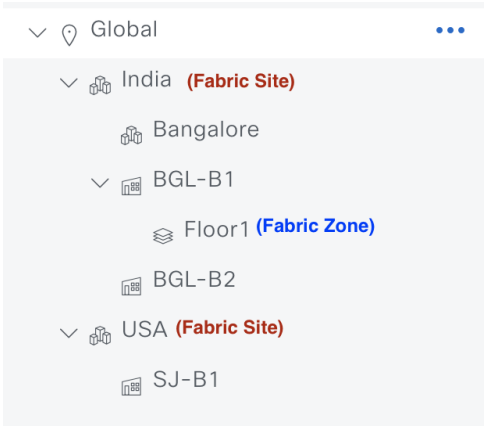


Table 52: Sample site move operations

Move operation	Allowed?	Reason
Move site *India* to new site *Asia* created under *Global*	Yes	You can move the site because the new parent or new ancestors are not fabric sites
Move site *India* under existing fabric site *USA*	No	You can't move a site under a new fabric site
Move building *BGL-B1* to *USA*	No	You can't move a building from one fabric site to another
Move building *BGL-B1* to new site *Asia* created under *Global*	No	You can't move a building out of a fabric site
Move floor *Floor1* to a new building *BGL-B2* within existing fabric site	Yes	You can move a zone within its fabric site
Move floor *Floor1* to a new building *SJ-B1* in a different fabric site	No	You can't move a zone to a different fabric site
Move building *BGL-B1* to *Bangalore*	Yes	You can move a building within the *India* fabric site

Configure a fabric site

After you create a fabric site, you can configure the devices, virtual networks, and authentication methods for the hosts to connect to a fabric site.

Select a fabric site under the **Provision** > **SD-Access** > **Fabric Sites** menu and use these tabs:

- **Fabric Infrastructure**: Assign devices to fabric roles.
- **Layer 3 Virtual Networks**: Create a Layer 3 virtual network for the fabric site or assign an existing Layer 3 virtual network to the fabric site.

- **Layer 2 Virtual Networks**: Create a Layer 2 virtual network for the fabric site or assign an existing Layer 2 virtual network to the fabric site.
- **Anycast Gateways**: Create an Anycast Gateway for a Layer 3 virtual network in the fabric site.
- **Authentication Template**: Select an authentication template for the fabric.
- **Wireless SSIDs**: Specify wireless SSIDs within the network that hosts can access. You can select the guest or enterprise SSIDs and assign address pools.
- **Port Assignment**: Apply specific configurations to each port, depending on the type of device that connects to the fabric site.

Each of these operations is explained in the later sections.



Note Constraints include:

- Cisco SD-Access deployments support only APs, extended nodes, user devices (such as a single computer or a single computer plus phone), and devices that need trunk ports, such as single servers.
- Servers with internal switches or virtual switches aren't supported.
- Other networking equipment (such as hubs, routers, or switches) isn't supported.

Add a device to a fabric

After you have created a fabric site, you can add devices to the fabric site. You can also specify whether the device should act as a control plane node, an edge node, or a border node.

You can add a new device to the fabric site only if IP Device Tracking (IPDT) is configured for the fabric site. To enable IPDT, go to **Design** > **Network Settings** > **Telemetry** and in the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button.

A device that is assigned the Access role and has been provisioned before enabling IPDT on the site can’t be added to the fabric. Reprovision such devices before adding them to the fabric site. Check the Provision workflow to confirm the status of **Deployment of IPDT** on the device.



Note

- It’s optional to designate the devices in a fabric site as control plane nodes or border nodes. You might have devices that don’t occupy these roles. However, every fabric site must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.
- Currently, the Cisco Wireless Controller communicates only with two control plane nodes.
- You cannot change a device's role after it is added to the fabric. To change the role, remove the device from the fabric and re-add it.

Before you begin

Provision the device if you haven't already provisioned it:

- The **Provision** > **Network Devices** > **Inventory** window displays the discovered devices.
- The topology view shows a device in gray if it has passed the fabric readiness checks and is ready to be provisioned.
- If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. Click **See more details** to check the problem area listed in the resulting window. Correct the problem and click **Re-check** to ensure that the problem is resolved.
- If you update the device configuration as a part of problem resolution, ensure that you resynchronize the device information by doing an **Inventory** > **Resync** for the device.



Note You can continue to provision a device that has failed the fabric readiness checks.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, click a device. A slide-in pane displays these **Fabric** options:

Option	Description
Edge Node	Toggle the button next to this option to enable the selected device as an edge node.
Border Node	Toggle the button next to this option to enable the selected device as a border node.
Control Plane Node	Toggle the button next to this option to enable the selected device as a control plane node.

To configure a device as a fabric-in-a-box, select the **Control Plane Node**, **Border Node**, and **Edge Node** options.

To configure the device as a control plane and a border node, select both **Control Plane Node** and **Border Node**.

Step 5 (Optional) To enable the wireless capability for the device, under **Capability**, click the **Embedded Wireless LAN Controller** toggle button and do these steps:

Alternatively, if the toggle button is already enabled, you can click **Configure** to configure the wireless settings.

a) If you have not installed the wireless package on the device yet, Catalyst Center displays a warning message indicating that the embedded wireless controller software image is necessary for enabling the capability. In the warning dialog box, click **OK** to install the image manually.

b) Under **Download Image**, click **Choose File** to navigate to a software image stored locally, or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.

c) Click **Import**.

The progress of the image import is displayed. To exit the window, and view the progress of the import and schedule the installation later, click **Close**.

d) After the image import is complete, under **Schedule Image Installation** on **Download Image**, choose one of these options:

- **Now**: Immediately install the image.
- **Later**: Schedule the image installation for a later date or time.

e) In the **Task Name** field, update the task name, if required.

f) If you chose **Later**, do these tasks:

- Under **Start Date/Time**, specify a start date and time for the image installation.
- To use the default site time zone for the image installation, check the **Site Settings** check box. To select a time zone, uncheck the **Site Settings** check box and choose a time zone from the drop-down list.

g) Click **Apply**.

To view the status of image installation, go to the **Activities** > **Tasks** window and open the relevant work item. After the software image is distributed and activated on the switch, you must resynchronize the device using the **Provision** > **Inventory** > **Resync** option.

h) Under **Manage Scope**, assign the managed AP locations for the embedded wireless controller:

- Under the **Primary** tab, check the check box next to the required site name.
- Under the **Secondary** tab, check the check box next to the required site name.

You can select either a parent site or individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

You can also use the **Search Hierarchy** search field or the filter icon to find a site.

i) Click **Next**.

j) Under **Advanced**, configure the required settings.

- To enable the Rolling AP Upgrade feature, check the **Rolling AP Upgrade** check box.

  (Optional) If you check this check box, from the **AP Reboot Percentage** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

- To renew the Locally Significant Certificate (LSC) for the associated APs before its expiry, check the **AP LSC Certificate Renewal** check box.

  If you check this check box, complete these configurations:

  - From the **Renewal Profile** drop-down list, select an AP LSC renewal profile.

    To create an AP LSC renewal profile, see Create an AP LSC renewal profile, on page 419.

  - (Optional) If you select an AP LSC renewal profile for staggered renewal, from the **AP Reboot %** drop-down list, select the percentage of APs that can be rebooted with minimal client disruptions. The default value is 25%.

Note If configured, the same AP reboot percentage value applies to both the Rolling AP Upgrade and staggered AP LSC renewal processes. For example, if you set the AP reboot percentage to 25%, only 25% of APs will reboot at a time during both Rolling AP Upgrade and staggered AP LSC renewal.

k) Click **Next**.
l) Under **Summary**, review the configuration settings.
m) Click **Save**.

If the wireless capability is enabled for a device and there are changes in the wireless network settings, to push the changes to the device, you must click **Configure** and save the configuration.

Step 6 Click **Add** to save the configurations.

Step 7 Click **Deploy** under the **Fabric Infrastructure** tab to configure the device.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note A device is added to the fabric only if the device runs a software release that is compatible with the Catalyst Center release. For information about fabric device compatibility, see Cisco SD-Access Compatibility Matrix.

For a given fabric role, if the software image on the device isn't compatible with the Catalyst Center release, the device isn't added to the fabric and an error message is displayed.

Step 9 On the **Tasks** window, monitor the task deployment.

What to do next

After a device is added to the fabric, fabric compliance checks are automatically performed to ensure that the device is fabric-compliant. The topology displays a device that has failed the fabric compliance check in blue color with a cross-mark beside it. Click **See more details** on the error notification to identify the problem area and correct it.

Remove a device from a fabric

Use this procedure to remove one or more devices from a fabric site.

Note If a border node in a fabric site is associated with a service insertion site, remove the association with the service insertion site to remove the device from the fabric site. For information, refer to Edit a service insertion site, on page 1165.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, choose the fabric site.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, choose a device that is part of the fabric (has a **Fabric Role**) using one of these options:

- Click the device name.
- Check the check box for the device and choose **More Actions** > **Edit Fabric Role**. You can choose multiple devices.

In the topology view, any device that is added to the fabric is shown in blue.

Step 5 In the slide-in pane, under the **Fabric** tab, click **Remove From Fabric**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

What to do next

After the task deployment succeeds, we recommend that you reboot each switch if you use an Embedded Wireless Controller on a Cisco Catalyst 9000 Series Switch with the wireless role enabled. Rebooting ensures optimal functionality. For example, if there are multiple Catalyst 9000 Series switches with the wireless role enabled in the same fabric site and you do not reboot, issues such as mobility tunnel limitations may occur.

To reboot each switch, complete these steps:

1. In the **Fabric Infrastructure** tab, click the switch name.
2. In the slide-in pane, click **Reboot**.
3. In the **Warning** dialog box, click **Yes**.

Add a device as a border node

When you add a device to a fabric, you can add it in various combinations to act as a control plane node, border node, or edge node, as described in Add a device to a fabric, on page 1022.

This section describes how to add a device as a border node and do these configurations:

- Border node type: Internal, External, or Internal and External (Step 9, on page 1027)
- Border node Priority (Step 10, on page 1028)
- Border node Affinity-ID (Step 10, on page 1028)
- TCP MSS Adjustment value on the border node switched virtual interfaces (SVIs) (Step 10, on page 1028)
- AS Path Prepend (Step 10, on page 1028)
- Associated transit: SD-Access transit or IP-based transit (Step 11, on page 1029)
- IP address pool allocation for Layer 3 handoff (Step 11, on page 1029)

Before you begin

To use the Border Node Affinity-ID feature, ensure that you create an SD-Access LISP Pub/Sub transit. For more information, see Create an SD-Access transit, on page 1033. When adding the first control plane node in the local fabric site, ensure that you select the LISP Pub/Sub control plane protocol. For more information, see Configure LISP Pub/Sub, on page 1030. The border node must be running Cisco IOS XE Release 17.8.1 or later.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, select the fabric site to configure a border node.
The resulting topology view displays all the devices in the network inventory. In the topology view, any device that is operating in a fabric role is shown in blue.

Step 4 Under the **Fabric Infrastructure** tab, click a device.

Step 5 In the slide-in pane, click the **Border Node** toggle button.

Step 6 In the resulting slide-in pane, click the **Layer 3 Handoff** tab.

Step 7 Check the **Enable Layer 3 Handoff** check box.

Step 8 Enter the **Local Autonomous Number** for the device.

If the local autonomous number is already configured on the device, this field displays the configured number and is disabled. You cannot change the local autonomous number if it's already configured on the device.

Step 9 Configure the type of border node. By default, a border node is designated as an external border node, wherein it acts as the default gateway to the fabric site, without importing any external routes.

A border node can be configured to be an internal border node, wherein it isn't the default gateway and only imports external routes. A border node can also have a combined role of internal and external borders.

- Check both the **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an external border node.
- Uncheck both the **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an internal border node.
- Check the **Default to all virtual networks** check box to designate the border node as an external and internal border. It acts as the fabric default gateway and also imports BGP-learned routes into the fabric site. (Don't check the **Do not import external routes** check box.)

For information about border node types, see the Cisco SD-Access Solution Design Guide.

Step 10 To configure the border node priority, affinity-ID, AS Path Prepend, TCP MSS adjustment and native multicast across SD-Access transit, click **Advanced** and do this configuration:

a) To change the border node priority, check the **Modify Border Priority** check box and enter a new priority value.

- Priority value ranges from 1 to 10.
- 1 indicates the highest priority.
- 10 indicates the lowest priority.
- The default priority value is 10.

If two or more border nodes are configured in a fabric site, traffic is routed through the border node that has a higher priority. If the priority values are the same, traffic is load balanced across the border nodes.

b) (Optional) To configure the border node affinity-ID, check the **Modify Border Node Affinity-ID** check box and enter values for these fields:

- **Affinity-ID Prime**: A lower relative prime value indicates a higher preference.
- **Affinity-ID Decider**: When the prime value is the same for two border nodes, the decider value is used as a tie-breaker to determine the border node preference.

Affinity-ID is a relative value, considering the value of this border node among the received values from all the other available border nodes. The lower the relative value of affinity-ID, the higher the preference for a destination border node. By default, the affinity-ID value isn't provisioned.

When the received affinity-ID values are equal, priority is used to determine the border node preference.

Note For proper functionality of the Affinity-ID feature, ensure that you configure an affinity-ID on all border nodes connected to the same SD-Access transit.

c) To define the number of AS Path prepends to the BGP AS_PATH list, check the **AS Path Prepending** check box and enter a value between 1 to 10.

AS Path prepending helps you to choose the ingress border.

d) To customize the TCP maximum segment size (MSS) value for the Layer 3 handoff SVIs, check the **TCP MSS Adjustment** check box and input the required value.

The TCP MSS Adjustment value can range from 500 to 1440. **TCP MSS Adjustment** value is applicable for the TCP sessions over both IPv4 and IPv6.



Note You can customize the TCP MSS value only if the border device is configured for Layer 3 handoff.

e) For an IPv6 underlay border, you can configure a custom identifier for the BGP router. Select the **Custom BGP Router ID** check box and enter the required value. The value must be in IPv4 format.

f) (Optional) To configure native multicast over multiple sites that are connected to an SD-Access transit, check the **Enable Multicast over SD-Access Transit** check box.



Note Ensure that you enable a similar check box for the SD-Access transit too.

You can view the border node priority and affinity-ID deployment logs in **Activities** > **Audit Logs**.

Step 11 Hover your cursor over **Add Transit Site** and select a transit that will be connected to this border node.

In an **IP:BGP IP TRANSIT**, you can choose to either automate the IP address allocation for a virtual network or manually assign the Local and Peer IP addresses for a virtual network. You cannot do both.

a) (Optional) To enable Catalyst Center to allocate IP address for the connection between the border node and peer, choose an IP address pool from the **Select IP Address Pool** drop-down list.



Note **Select IP Address Pool** is disabled if you have manually assigned the Local and Peer IP addresses.

b) To configure the handoff interface, click **Add External Interface**.

Do these steps in the resulting window:

1. Select an interface from the **External Interface** drop-down.
2. The **Remote AS Number** is automatically derived from the selected Transit or Peer network.
3. (Optional) Enter the a description for the interface in the **Interface Description** field.
4. (Optional) From the **Actions** drop-down list, choose **Enable All** or **Disable All**.
5. Click the **Enable Layer 3 Handoff** toggle button for the virtual network. This virtual network is advertised by the border node to the peer through BGP. You can select one, multiple, or all virtual networks.
6. In the **VLAN ID** field, enter an ID for the selected virtual network.
7. (Optional) To manually assign the IPv4 and IPv6 **Local IP Address** and **Peer IP Address** for the selected virtual network, enter the IP addresses and subnet mask in the CIDR notation (IP address/prefix-length).



Note The **Local IP Address** and **Peer IP Address** fields are disabled if you have already selected an IP Pool.

8. Click **Save**.

c) Click **Add**.

When configuring an SDA transit, you can enable dual-stack support on the external border node. Follow these steps:

a) Click the **Advanced attributes** toggle button.
b) Select the **Dual stack RLOC registration** check box.
c) Choose the underlay IP address type to connect the SDA transit—**IPv4** or **IPv6**.

Step 12 (Optional) Perform this step only if you are connecting a traditional network to the fabric site or you are migrating from a traditional network to an SD-Access network. Click the **Layer 2 Handoff** tab.

A list of virtual networks and the count of IP address pools in each virtual network displays.

a) Click a virtual network that is to be handed off.

A list of IP address pools that are present in the virtual network and a list of interfaces through which you can connect to the traditional network displays.

b) From the **External Interface** drop-down, choose an interface.
c) Under **Interface Description**, enter an optional description for the interface.
d) In the **External VLAN** field, enter the VLAN number into which the fabric must be extended.

A virtual network can be handed off on a single interface or on multiple interfaces. Layer 2 handoff for a segment can also be done on two different devices. In both cases, ensure that no loops are formed in the network.

Because a border node is connected to the traditional network, it is subject to broadcast storms, Layer 2 loops, and spanning-tree problems that can occur in Layer 2 switched access networks. To prevent disruption of control plane node services or border node services connecting to other external networks, a border node should be dedicated to the Layer 2 handoff feature and not colocated with other fabric roles or services.

e) Click **Save**.

Step 13 Click **Add** to save the configurations.

Step 14 Click **Deploy** under the **Fabric Infrastructure** tab to configure the border node.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note A device is configured as a border node only if the device runs a software release that is compatible with the Catalyst Center release. If the device runs an incompatible software, an error message is displayed and the device is not configured as a fabric border node. For information about software compatibility, see the Cisco SD-Access Compatibility Matrix.

Step 15 On the **Tasks** window, monitor the task deployment.

Configure LISP Pub/Sub

You can configure LISP Pub/Sub on a fabric site only when you add the first control plane to your fabric.

Before you begin

Ensure that the fabric devices operate on Cisco IOS XE Release 17.6.1 or later.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Choose the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, click a device that is to be configured as a control plane.

Step 5 In the slide-in pane, enable the **Control Plane Node** toggle button to configure this plane.

Step 6 In the **Configure Control Plane** slide-in pane, choose **LISP Pub/Sub** route distribution protocol and click **Add**.

Step 7 Click **Deploy** under the **Fabric Infrastructure** tab to configure the LISP Pub/Sub Control Plane.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Step 9 To verify the configuration of LISP Pub/Sub in the fabric site, see the LISP Pub/Sub status on the **SITE SUMMARY** window.

Reconfigure a fabric

If you modify an IP address pool that is used in a fabric, the fabric becomes outdated. Use this procedure to update the fabric to configure the IP address pool changes to the devices in the fabric site.

The time taken to the reconfigure the fabric depends on the number of devices.



Note You can't perform other operations on the fabric devices until the fabric is reconfigured to update the devices with the IP address pool changes.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, select the fabric site that uses the modified IP address pools.

Step 4 In the **Fabric Infrastructure** tab, under the warning alert, click **Reconfigure Fabric**.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 5 On the **Tasks** window, monitor the task deployment.

Create an IP transit

Use this procedure to create an IP transit.

Procedure

Step 1 From the main menu, choose **Workflows** > **Create Transits**.

Alternatively, you can navigate to **Provision** > **Transits**, and click **Create Transit**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Transit Name and Type** window, do these steps:

a) In the **Transit Name** field, enter a name for the transit.

b) From the **Transit Type** drop-down list, choose **IP-Based**.

The routing protocol is set to BGP by default.

c) In the **Remote BGP Autonomous System Number** field, enter the Autonomous System Number (ASN) for the transit.

d) Click the **Advanced attributes** toggle button to enable or disable the advanced attributes.

e) In the **Select Site** drop-down list, choose a site for the transit.

Ensure that the chosen site is at the fabric site level or above it.

You can edit the site mapping after creating the transit. To edit, in the **Transits** window, click **More Actions** > **Edit Transit** and update the site selection as required.

If the transit is...	Then...
associated with fabric sites	choose a site that is a common parent for all the associated fabric sites.
not associated with fabric sites	you can choose any site that is at a level of a fabric site or above it.

Step 4 In the **Transit Control Plane Nodes** window, click **Next**.

Step 5 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Create an SD-Access transit

Use this procedure to create an SD-Access transit.

Procedure

Step 1 From the main menu, choose **Workflows** > **Create Transits**.

Alternatively, you can navigate to **Provision** > **Transits** and click **Create Transit**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Transit Names and Types** window, do these steps:

a) In the **Transit Name** field, enter a name for the transit.

b) From the **Transit Type** drop-down list, choose a transit type.

- To configure a transit for the fabric sites that don't have a LISP Pub/Sub control plane, choose **SD-Access (LISP/BGP)**.
- To configure a transit for the fabric sites that have a LISP Pub/Sub control plane, choose **SD-Access (LISP Pub/Sub)**.

  If you choose this option, to enable native multicast over the transit, check the **Native Multicast Over SD-Access Transit** check box.

  Note To complete the native multicast configuration over multiple sites that are connected to the SD-Access transit, ensure that you enable multicast over SD-Access transit on the border nodes.

  To share the **SD-Access (LISP Pub/Sub)** transit with other Catalyst Center clusters, choose **Yes, Share**. Otherwise, choose **No, keep it local**.

Note The **Yes, Share** option is visible only if the **Multiple Catalyst Center** package is installed on all the Catalyst Center clusters.

c) Toggle on **Advanced attributes** and in the **Site** drop-down list, choose a site for the transit.

Ensure that the chosen site is at a level above the fabric site. By default, it's set to *Global*.

You can edit the site mapping after creating the transit. To edit, in the **Transits** window, click **More Actions** > **Edit Transit** and update the site selection as required.

If the transit is...	Then...
associated with fabric sites	choose a site that is a common parent for all the associated fabric sites and the associated transit control plane nodes.
not associated with fabric sites	you can choose any site that is a common parent for the associated transit control plane nodes.

Step 4 In the **Transit Control Plane Nodes** window, do these steps:

a) From the **Select a Site** drop-down list, choose a site with a control plane node.

Note You can't add an **SD-Access (LISP Pub/Sub)** transit to a fabric site that uses the LISP/BGP control plane. You can't add **SD-Access (LISP/BGP)** transit to a fabric site that uses the LISP Pub/Sub control plane.

b) From the **Transit Control Plane Node** drop-down list, choose a control plane node.

c) (Optional) To configure an additional node, click the plus icon and repeat 4.a, on page 1034 and 4.b, on page 1034.

Step 5 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

What to do next

To interconnect the fabric sites with an SD-Access transit, add the transit to the fabric border node.

Configure an authentication template for the fabric site

Use this procedure to configure an authentication template that applies to all devices in the fabric site.

Note If one or more stack members or line cards are added on any of the existing switches in the fabric, a warning alert is displayed to configure the authentication template on these new stack members or line cards as well. Click **Apply Fix** in the warning alert to apply the configurations and update the fabric.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Click a fabric site.

Step 4 Click the **Authentication Template** tab.

Step 5 Under **Select Authentication Template**, choose an authentication template for the site.

- **Open Authentication**: A host is allowed network access without having to go through 802.1X authentication.
- **Closed Authentication**: Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.
- **Low Impact**: Security is added by applying an ACL to the switch port to allow limited network access prior to authentication. After a host is successfully authenticated, additional network access is granted.
- **None**

For **Closed Authentication**, **Open Authentication**, and **Low Impact** templates, you can configure the following settings:

- **Voice VLAN**: Use this check box to enable or disable the default voice VLAN (VLAN 2046) for the site.
- **BPDU Guard** (**Closed Authentication**): Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.

You can edit the settings of the chosen authentication template to address site-specific authentication requirements.

Before you change the site-level authentication, you must resynchronize any fabric device whose APs were onboarded through macros or autoconf and haven't yet undergone the periodic resync.

Step 6 (Optional) To edit the settings of the chosen authentication method, click **Edit**.

a) In the slide-in pane, edit the required settings.

- **First Authentication Method**: Choose **802.1x** or **MAC Authentication Bypass (MAB)**
- **802.1x Timeout (in seconds)**: Use the slider to specify the 802.1x timeout, in seconds.
- **Wake on LAN**: Choose **Yes** or **No**.

  Wake on LAN (WoL) is supported only when

  - the source (WoL initiator) and destination (sleeping host) are both in the same subnet, and Layer 2 Flooding is enabled; or

- the source is outside the SD-Access fabric but located in the network that is connected to the fabric through Layer 3 handoff. The destination is in an SD-Access subnet with IP-Directed Broadcast enabled.

Note These topologies do not support WoL:

- The WoL initiator and the sleeping host are on different subnets within the same Layer 3 Virtual Network.
- The WoL initiator routes to the sleeping host over an SD-Access Transit.

- **Number of Hosts**: Choose **Unlimited** or **Single**.

Note **Number of Hosts** specifies the number of data hosts that can be connected to a port. With **Single**, you can have only one data client on the port. With **Unlimited**, you can have multiple data clients and one voice client on the port.

- **Pre-Authentication Access Control List**: Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

b) Click **Save**.

The saved modifications apply only to the site for which the authentication template is edited.

Step 7 Click **Deploy** under the **Select Authentication Template** tab to configure the authentication template for all the nodes.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

The Hitless Authentication Change feature lets you switch from one authentication method to another without removing the devices from the fabric.

Step 8 On the **Tasks** window, monitor the task deployment.

Configure ports within the fabric site

The **Port Assignment** tab enables you to configure each access device in the fabric site. You can specify network behavior settings for each port on a device.

If you don't configure the authentication template for an individual port, the port inherits these settings from the global authentication template configuration. An inherit icon displays next to the authentication template name for the corresponding port in the **Ports** table.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, click a fabric site to configure the port assignments.

Step 4 Click the **Port Assignment** tab.

Step 5 From the list of fabric devices, select a device and click **Configure**.

Step 6 In the **Configure Port Assignments** slide-in pane, click a type of connected device:

Option	Description
User Devices and Endpoints	Configures the port to connect to a host device.
Access Point (AP)	Configures the port to connect to an access point.
Trunk	Configure the port as a trunk port.
Supplicant-Based Extended Node	Configures the port to receive a supplicant-based extended node.

- To connect host devices, click **User Devices and Endpoints** and do these steps:
  a. Choose the VLAN name for data from the **VLAN Name (Data)** drop-down list.
  b. Choose a security group from the **Security Group** drop-down list.
     Security groups are supported only with the **None** authentication template.
  c. Choose the VLAN name for voice from the **VLAN Name (Voice)** drop-down list.
  d. Choose the authentication type from the **Authentication Template** drop-down list.
  e. Enter a **Description** for the connected device.

- To connect an access point, click **Access Point** and do these steps:
  a. Choose the VLAN name from the **VLAN Name (Data)** drop-down list.
  b. Choose the authentication type from the **Authentication Template** drop-down list.
  c. Enter a **Description** for the connected device.

- To connect a supplicant-based extended node device, click **Supplicant-Based Extended Node**.
- To connect a trunk port, click **Trunk** and enter a **Description** for the port.
  Configure **Native VLAN** and **Allowed VLANs** for the trunk port.
  - In the **Native VLAN** field, enter a value for the native VLAN.
    The valid range is from 1 to 4094. The default value is 1.

- In the **Allowed VLANs** field, you can choose to allow all VLANs, a specific VLAN ID between 1 and 4094, or specify a range of VLANs. For example, you can enter 100, 200, or 300-400. The default value is **All**.

Note When templates override default values, update the trunk configuration to align with the values that are specified for each port in the template.

Step 7 Click **Update** in the **Configure Port Assignment** slide-in pane to save the configurations.

Step 8 Click **Deploy All** under the **Port Assignment** tab to update the port assignments.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure wireless SSIDs for fabric networks

Before you begin

Ensure to add the wireless device to the fabric site.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Click a fabric site.

Step 4 Click the **Wireless SSIDs** tab and specify the wireless SSIDs within the network that the hosts can access.

Step 5 From the **Choose Pool** drop-down list, choose an IP address pool reserved for the SSID.

The wireless IP address pools that are configured for Layer 3 and Layer 2 segments are available in this drop-down list.

Step 6 From the **Assign SGT** drop-down list, choose a security group for the SSID.

Step 7 Check the **Enable Wireless Multicast** check box to enable wireless multicast on the SSIDs.

Step 8 Click **Deploy**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure a wireless mesh access point in a fabric

Starting with Catalyst Center Release 2.3.7, you can onboard a wireless Mesh AP in an SD-Access fabric. You can provision a mesh AP either as a Mesh Access Point (MAP) or a Root Access Point (RAP), depending on the network requirement. For more information, see About Wireless Mesh Networks.

Before you begin

- Define a list of authorized Access Points (APs). You can choose the AP authorization list while provisioning the Cisco Wireless Controller. Cisco Wireless Controllers respond only to requests from those APs that are present in the AP authorization list. For information on how to create a list of authorized APs, see Create an AP Authorization List.
- Define an AP Profile to manage and provision the mesh AP. See Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices.

Procedure

Step 1 If you have existing APs that you want to use in the mesh network mode, you must first change the AP Mode to Bridge using the **Configure Access Point** workflow. For information, see Configure APs.

Step 2 Provision the fabric-enabled wireless controller with the AP Authorization List to onboard the Mesh APs. See Provision a Cisco Catalyst 9800 Series Wireless Controller.

What to do next

Onboard an AP and provision it in the role of a MAP or a RAP.

Configure security service insertion on a fabric site

Use this procedure to configure service insertion on a fabric site.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, select the fabric site for which you want to configure security service insertion.

Step 4 In the corresponding fabric site window, hover your cursor over **Site Actions** and choose **Enable Service Insertion**.

Step 5 Complete these configurations to enable service insertion site on this fabric site.

If service insertion site is...	Then...
not yet enabled on any fabric site	see Prechecks to enable a service insertion site on day zero, on page 1162 to enable security service insertion.
already enabled on another fabric site	see Enable a service insertion site, on page 1164 to configure this fabric site as a service insertion site.
already enabled on this site	see Edit a service insertion site, on page 1165 to edit the service insertion site configurations.

Virtual networks

Virtual networks are overlays that are used to segment traffic within a common physical network infrastructure; this is also known as macrosegmentation. Layer 2 virtual networks segment switched traffic, and Layer 3 virtual networks segment routed traffic. Each endpoint that is connected to a Cisco SD-Access fabric is assigned to a specific virtual network based on the static edge port configurations or the dynamic policy from the Cisco Identity Service Engine. Within a virtual network, endpoints can communicate with each other unless explicitly blocked by microsegmentation policy. Endpoints across different virtual networks cannot communicate with each other by default. Intervirtual network traffic requires connectivity policy to be implemented outside of the Cisco SD-Access fabric, such as on a fusion device.

A typical use case for virtual networks is an office building containing both corporate endpoints and building-management systems. The corporate endpoints must be segmented from building systems, such as lighting, heating, ventilation, and air conditioning. In such a scenario, a network administrator can use macrosegmentation to segment the corporate endpoints and the building systems using two or more virtual networks to block unauthorized access between the building systems and corporate endpoints.

A Layer 3 virtual network may span multiple fabric sites and across network domains (wireless LAN, campus LAN, and WAN). A Layer 2 virtual network resides within a single fabric site.

Create a Layer 3 virtual network

Procedure

Step 1 From the main menu, choose **Workflows** > **Create Layer 3 Virtual Networks**.

Alternatively, you can navigate to the **Layer 3** tab in **Provision** > **Virtual Networks** and click **Create Layer 3 Virtual Networks**.

Step 2 If the task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 3 In the **Layer 3 Virtual Networks** window, do these steps:

a) In the **Layer 3 Virtual Network name** field, enter a name for the Layer 3 virtual network.

b) (Optional) To create another Layer 3 virtual network, click the plus icon and enter a name for the Layer 3 virtual network.

Step 4 In the **Fabric Sites and Fabric Zones (Optional)** window, do this configuration:

a) Click **Select Fabric Sites** and choose the fabric sites.

You can assign a virtual network to multiple fabric sites. To choose the fabric sites, do one of these tasks:

- Click the plus icon next to the required fabric sites.
- Click the fabric site name and click **Add Selected**.

Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

- To choose all the fabric sites, click **Add All**.

Repeat this association for all the Layer 3 virtual networks that you created.

b) Click **Assign**.

c) Click **Select Fabric Zones** and do one of these tasks:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

d) Click **Assign**.

Step 5 Review the Layer 3 virtual network settings in the **Summary** window.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Create a Layer 2 virtual network

Procedure

Step 1 From the main menu, choose **Workflows** > **Create Layer 2 Virtual Networks**.

Alternatively, you can navigate to the **Layer 2** tab under **Provision** > **Virtual Networks** and click **Create Layer 2 Virtual Networks**.

Step 2 If the task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 3 In the **Configuration Attributes** window, configure the required Layer 2 virtual network attributes.

a) In the **VLAN Name** field, enter the VLAN name.

b) In the **VLAN ID** field, enter the VLAN ID. The valid range for VLAN ID is from 2 through 4093.

Note The VLAN IDs from 1002 through 1005 and 2046 are reserved VLAN IDs.

c) From the **Traffic Type** area, choose **Data** or **Voice**.

d) Check the **Fabric-Enabled Wireless** check box to enable wireless.
The **Layer 2 Flooding** check box is enabled by default for a Layer 2 virtual network.

e) For **Layer 2 Flooding**, you can choose the flooding address type and assign a custom flooding IP address, if required.

- **Flooding Address Assignment**: Choose Shared or Custom.
- **Flooding Address**: If you chose Custom, enter a flooding IP address for the Layer 2 flooding—the supported IP address ranges are 239.0.0.0/8 for IPv4 and FF30::/96 for IPv6. You cannot edit the flooding address for a Shared address type.

Layer 2 Flooding is supported on anchored and inherited virtual network in these ways:

- If **Layer 2 Flooding** is disabled on anchored virtual network, it is disabled on inherited virtual network as well.
- If **Layer 2 Flooding** is enabled on anchored virtual network, it can be enabled or disabled on the inherited virtual network. If it is enabled, the flooding address assignment type and the flooding address must be same as the anchored virtual network.

f) Check the **Flood Access Tunnel** check box, to enable flood access tunnel. It is enabled by default for a Layer 2 virtual network if **Fabric-Enabled Wireless** is enabled.

g) Check the **Resource Guard** check box to block the SSDP traffic in the fabric.

h) To add another Layer 2 virtual network, click the plus icon and repeat 3.a, on page 1042 to 3.d, on page 1042.

Step 4 In the **Fabric Sites and Advanced Attributes** window, choose a fabric site for the Layer 2 virtual network from the **Fabric Sites** drop-down. Optionally, you can follow these steps to choose the fabric zone to associate with this Layer 2 virtual network:

a) Click **Select Fabric Zones** and choose one of these options to add the fabric zones:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Repeat this association for all the Layer 2 virtual networks that you created.

Step 5 (Optional) In the **Fabric Sites and Advanced Attributes** window, click the **Advanced Attributes** toggle button on to associate a Layer 3 virtual network to this Layer 2 virtual network.

Step 6 In the **Summary** window, review your Layer 2 virtual network settings.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Step 9 After you see a success message, click **View Anycast Gateway** to verify the gateway creation.

In the **Virtual Networks** window, the **Anycast Gateway** tab displays the details of all the anycast gateways in the fabric.

Associate Layer 3 virtual networks to fabric sites

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Layer 3 Virtual Networks**.

The resulting window displays all the Layer 3 virtual networks that are created at the global level.

Step 3 In the **Layer 3** tab, check the check box next to the Layer 3 virtual networks for which you want to edit the fabric site association.

Note You can edit up to five Layer 3 virtual networks.

Step 4 Hover your cursor over **More actions**, and choose **Edit Fabric Site and Fabric Zone Associations**.

Step 5 In the **Fabric Sites and Fabric Zones (Optional)** window, do this configuration:

a) Click **Select Fabric Sites** and choose the fabric sites.

You can assign a virtual network to multiple fabric sites. To choose the fabric sites, do one of these tasks:

- Click the plus icon next to the required fabric sites.
- Click the fabric site name and click **Add Selected**.



Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

- To choose all the fabric sites, click **Add All**.

Repeat this association for all the Layer 3 virtual networks.

b) Click **Assign**.

c) Click **Select Fabric Zones** and do one of these tasks:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.



Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

d) Click **Assign**.

Step 6 Review the Layer 3 virtual network sites on the **Summary** window.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Create anycast gateways

Before you begin

Ensure that you have created a Layer 3 virtual network. For more information, see Create a Layer 3 virtual network, on page 1040.

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Anycast Gateways**.

Step 3 In the **Anycast Gateway** tab, click **Create Anycast Gateways**.

Alternatively, click the menu icon and choose **Workflows** > **Create Anycast Gateways**.

Step 4 If the task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 5 In the **Layer 3 Virtual Networks** window, select one or more virtual networks to add a gateway.

- Click the plus icon next to the required fabric sites.
- Click the fabric site name and click **Add Selected**.



Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

- Click **Add All** to choose all the fabric sites.

Step 6 In the left pane of the **Configuration Attributes** window, choose the Layer 3 virtual network for which you want to create the anycast gateway and configure the required attributes.

a) From the **IP Address Pool** drop-down list, choose an IP address pool.

You can configure secondary IP address pools for the anycast gateway.

- To add secondary IP pools,
  1. Click **Add additional IP addresses pool**.
  2. In the **Select IP Pools** window, select up to four additional IP address pools and click **Save**.
- To edit a secondary IP pool,
  1. Click **Edit additional IP address pools**.
  2. Edit or delete the IP address pools as required and click **Save**.



Note When creating anycast gateways in the INFRA_VN, dual-stack IP address pools (containing both IPv4 and IPv6 addresses) are not supported. Select a single-stack IP address pool that corresponds to the fabric underlay type: use an IPv4-only pool for IPv4 underlay fabrics or an IPv6-only pool for IPv6 underlay fabrics.

b) For INFRA_VN, configure these attributes:

- Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.
- Enter a custom **VLAN ID** for the virtual network.

- Under **Pool Type**, select either **Fabric APs** or **Extended Nodes**.

If you select...	Then...
Fabric APs	Check the **MACsec Encrypted** check box to enable MACsec encryption of AP uplink traffic for supported APs. Catalyst Center supports MACsec configuration on switches in the fabric edge role for these platforms: Cisco Catalyst 9300, 9500, and 9500H Series Switches. If a fabric site contains a Cisco Catalyst 9350 Series Smart Switch, you cannot enable MACsec for that fabric site. **Note** Before you enable MACsec encryption for AP uplink traffic, ensure that the Cisco ISE AP onboarding authorization profile returns the required MACsec attributes to the access switch. For more information, refer to Configure Cisco ISE for fabric AP MACsec on edge nodes, on page 1049. For information about applicable APs, refer to *Feature Matrix for Cisco Wireless Access Points*.
Extended Nodes	• Check the **Supplicant-Based Extended Node Onboarding** check box to onboard a supplicant-based extended node. • Check the **MACsec Encrypted** check box for MACsec encrypted onboarding of supplicant-based extended node. **Note** The **MACsec Encrypted** check box is active only when you select the **Supplicant-Based Extended Node Onboarding** option.

- Use the **Enforcement** check box to enable or disable the enforcement of group-based policy for your network. The **Enforcement** check box is selected by default.

Note The option to disable the enforcement of group-based policies can be useful while onboarding devices in networks that have a default policy set to deny. The **Enforcement** option will not be available after the check box has been unchecked.

c) Check the **IP-Directed Broadcast** check box to enable the IP-Directed Broadcast feature.

Note

- When you enable Directed Broadcast, Catalyst Center automatically enables Layer 2 flooding.
- Routers and Cisco Nexus 7000 Series Switches don't support Directed Broadcast.
- Before enabling Directed Broadcast, ensure that you have enabled underlay multicast.

d) Check the **Intra-Subnet Routing** check box to enable the intrasubnet routing.

Note When you enable intrasubnet routing, Catalyst Center automatically disables the **Fabric-Enabled Wireless** and **Layer 2 Flooding** check boxes.

e) Check the **TCP MSS Adjustment** check box and input the required value to customize the TCP maximum segment size (MSS) value for the anycast gateway.

You can set a **TCP MSS Adjustment** value between 500 and 1440. This value applies to TCP sessions over both IPv4 and IPv6.

TCP MSS Adjustment value is applied to all the anycast gateway switched virtual interfaces (SVIs).

f) Check the **Silent Host Discovery** check box to enable silent host detection on the anycast gateway.

To enable silent host detection with Pre-Auth VLANs, click **Edit Pre-Auth VLANs**. In the Edit window, select the Pre-Auth VLANs. If you are using a custom Pre-Auth VLAN (other than VLAN 1), create an anycast gateway with **Candidate Pre-Auth VLAN** enabled (see *Step l*).

Note To allow pre-authenticated traffic flow for **Silent Host Discovery** with Pre-Auth VLANs, ensure that the authentication template for the fabric is in open, closed, or low impact mode with **Authentication Control Direction** set to **In**.

g) Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.

h) Enter a custom **VLAN ID** for the virtual network.

Note
- VLAN IDs 1, 1002-1005, 2046, and 4095 are reserved and can't be used.
- If you don't provide a custom VLAN ID, Catalyst Center generates a VLAN ID in the range of 1021–2020.

i) Choose **Data** or **Voice** from the **Traffic Type** area.

j) From the **Security Group** drop-down list, choose a security group.

k) Check the **Critical VLAN** check box to include this IP pool in the critical IP address pool.

A critical pool is used for closed authentication profile when an authentication server isn't available. A critical VLAN is assigned to the critical pool and all unauthenticated hosts are placed in the critical VLAN in the absence of an authentication server.

Note When you enable critical VLAN, Catalyst Center automatically generates the VLAN name.

l) Check the **Candidate Pre-Auth VLAN** check box to enable the anycast gateway to be used as a Pre-Auth VLAN. Ensure to configure the VLAN ID when you enable this check box.

After you enable the **Candidate Pre-Auth VLAN**, the VLAN ID can be selected as a Pre-Auth VLAN while configuring the Silent Host Discovery feature.

m) Check the **Resource Guard** check box to block the SSDP traffic in the fabric.
n) Check the **Fabric-Enabled Wireless** check box to enable this IP pool as a wireless IP address pool.
o) Check the **Layer 2 Flooding** check box to enable Layer 2 flooding.

Note Layer 2 flooding requires underlay multicast, which is configured during LAN automation. If you don't provision the underlay through LAN automation, configure the underlay multicast manually.

p) For **Layer 2 Flooding**, choose the flooding address type and assign a custom flooding IP address if needed.

- **Flooding Address Assignment**: Choose Shared or Custom.
- **Flooding Address**: If you chose Custom, enter a flooding IP address for the Layer 2 flooding—the supported IP address ranges are 239.0.0.0/8 for IPv4 and FF30::/96 for IPv6. You cannot edit the flooding address for a Shared address type.

Layer 2 Flooding is supported on anchored and inherited virtual network in these ways:

- If **Layer 2 Flooding** is disabled on anchored virtual network, it is disabled on inherited virtual network as well.
- If **Layer 2 Flooding** is enabled on anchored virtual network, it can be enabled or disabled on the inherited virtual network. If it is enabled, the flooding address assignment type and the flooding address must be same as the anchored virtual network.

Note The **IP-Directed Broadcast** feature adopts the **Flooding Address Assignment** and **Flooding Address** configurations for Layer 2 flooding, if they are configured.

q) Check both the **Fabric Enabled Wireless** and the **Multiple IP-to-MAC Addresses** check boxes to enable onboarding of bridge-mode virtual machines that are connected to the fabric-enabled wireless network.
r) Check only the **Multiple IP-to-MAC Addresses** check box to enable a wired host to have multiple IPv4 addresses (IP aliasing).

You can have a maximum of 1000 IPv4 addresses for a single MAC address.

s) Check the **Flood Access Tunnel** check box, to enable flood access tunnel. You can use this option only when **Fabric-Enabled Wireless** is enabled.
t) Click the plus icon and repeat the steps to associate more IP pools.

Step 7 In the **Fabric Zones (Optional)** window, add the fabric zones.

a) Click **Select Fabric Zones** and choose one of these options to add the fabric zones:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- Click **Add All** to choose all the fabric zones.

b) Click **Assign**.

Step 8 Review the anycast gateway settings in the **Summary** window.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Configure Cisco ISE for fabric AP MACsec on edge nodes

Use this procedure to configure Cisco ISE for fabric AP MACsec on edge nodes. For more information, refer to *Cisco Identity Services Engine Administrator Guide*.

Fabric AP MACsec on edge nodes is MACsec encryption for AP uplink traffic between a fabric AP and the fabric edge node that the AP connects to.

For fabric AP MACsec on edge nodes, update the existing Cisco ISE AP onboarding authorization profile so that Cisco ISE returns the MACsec link-security policy and AP interface template attributes to the switch.

Procedure

Step 1 From the Cisco ISE main menu, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Configure these attributes for the **AP_FULL_ACCESS** authorization profile:

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = linksec-policy=should-secure
cisco-av-pair = interface-template-name=ApAutzTemplate
```

Step 3 Save the authorization profile.

Extranet policy

Configure an extranet policy to allow route leaks between Layer 3 virtual networks (VNs), without using a fusion device. Use an extranet policy to provide the endpoints (hosts or users) with access to shared services like DHCP, DNS, Internet, and so on, through Catalyst Center automation. The shared services connect to a Provider VN. The endpoints that use the shared services reside in a Subscriber VN. An extranet policy establishes communication between the Provider VN and the Subscriber VNs.

You can create an extranet policy, edit an extranet policy, and delete an extranet policy for these deployments:

- Single site fabric with IP Transit

- Multi-site fabric with SDA Transit

Extranet policy management

Catalyst Center supports a new CLI configuration for deploying extranet policies on border devices moving away from the legacy policy-based routing configurations. The new CLI configuration is supported on border devices that are running Cisco IOS XE Release 17.18.1 or higher only; devices running a lower version will continue to support policy-based routing configurations.

You can view the extranet policy status under the **Extranet Policy** column in the fabric site table. Use the settings option to enable the **Extranet Policy** column view in the table.

Extranet policy migration scenarios

Catalyst Center supports migration of a fabric site from policy-based routing configuration to the new CLI approach based on the border device support.

An information banner is displayed in the fabric window when the site is ready for migration.

Note After all the devices in a fabric are migrated to the new CLI-based extranet policy, you cannot revert to policy-based routing configurations or add any border device to the fabric that is running an IOS XE version lower than 17.18.1.

This table describes the migration scenarios for new and existing fabric sites.

For a new site, where all border devices in the fabric are on version equal to higher than 17.18.1.	Migration happens automatically. After the creation of extranet policy, it is deployed on all the border devices in the fabric using the new CLI configurations.
For an existing site, where all border devices in the fabric are upgraded to version equal to higher than 17.18.1.	An information banner is displayed indicating that the site is ready for migration and the updates can be applied.

Guidelines for configuring an extranet policy

Consider these guidelines before you configure an extranet policy:

- To configure an extranet policy, a device should operate Cisco IOS XE 17.9.1 or a later release.
- Extranet Policy is supported only on the fabric sites that have a LISP Pub/Sub control plane.
- To configure an extranet policy on a multisite fabric with SD-Access transit, ensure that all the sites have the provider VN.
- If you configure multiple VN policies in your network, the same VN cannot be the Provider VN in more than one policy.
- Extranet Policy does not support overlapping IP pools.
- Provider VN in a policy cannot be configured as a Subscriber VN in another VN Policy and conversely.
- Add the Provider VN to all the fabric sites where an extranet policy is applicable.

- Ensure that the Provider VNs do not leak into each other outside the fabric. Else, it might result in route leaks between the Subscriber VNs.
- Extranet policy is not supported on router devices.
- Inter-VN multicast through an extranet policy is not supported. You cannot route multicast between the Layer 3 virtual networks that are interconnected through an extranet policy.

Create an extranet policy

To create an extranet policy:

Procedure

Step 1 From the main menu, choose **Workflows** > **Create Extranet Policy**.

Alternatively, navigate to **Extranet Policies** tab under **Provision** > **Virtual Networks**. In the **Extranet Policies** window, click **Create Extranet Policy**.

Step 2 Follow the on-screen guidance to provide a name for the policy, to choose a provider VN and the subscriber VNs.

You can assign this extranet policy to one or more fabric sites.

In a multisite deployment where an SD-Access transit connects the fabric sites, ensure that you select all the fabric sites that are connected by the SD-Access transit.

Step 3 On the **Summary** page, review the extranet policy configuration.

To make changes, click **Edit** next to the group of settings that you want to change.

Step 4 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 5 On the **Tasks** window, monitor the task deployment.

Edit an extranet policy

You can edit an extranet policy to add or delete subscriber VNs and to assign or remove the policy from a fabric site.

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 In the **Extranet Policies** tab, select the policy to be edited, and click **More Actions** > **Edit Extranet Policy**.

Step 3 Follow the on-screen guidance to edit the policy.

Delete an extranet policy

To delete an extranet policy:

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 In the **Extranet Policies** tab, select the policy to be deleted, and click **More Actions** > **Delete Extranet Policy**.

Step 3 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 4 On the **Tasks** window, monitor the task deployment.

Configure a fabric zone

A fabric site (parent site) can be divided into fabric zones with smaller subnets to help you manage the network easily. A fabric zone can have its own edge nodes and extended nodes, but it connects to the parent site for a control plane and border. If you migrated from an earlier Catalyst Center release to the current release, you can create a fabric zone on the existing fabric site. This fabric zone inherits all the properties of its parent site.

Before you begin

- Ensure that you have created a network hierarchy under the Global site.
- Select a parent site that is not at the lowest level in the hierarchy.

The broad workflow to configure a fabric zone includes:

1. Create a fabric zone in one of these ways:
   - Create a fabric site and its zones using the **Create Fabric Site** workflow. For more information, see Create a fabric site and fabric zones, on page 1053.
   - Edit an existing fabric site to add fabric zones to it. For more information, see Create a fabric zone within a fabric site, on page 1054.
2. Add edge nodes and extended nodes to the fabric zone. For more information, see Add a device to a fabric, on page 1022.

3. Assign Layer 3 virtual networks and segments to the fabric zone. For more information, see Associate Layer 3 virtual networks to fabric zones, on page 1055.

Note Only the virtual networks and segments of the parent site are available to the fabric zone.

Note After a segment is added to a fabric zone, it can't be updated in the parent site.

You can't edit edge nodes and extended nodes of a fabric zone in its parent site.

You can configure the edge node of a fabric zone as a control plane or a border of the parent site.

Create a fabric site and fabric zones

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Click **Create Fabric Site**.

Alternatively, click the menu icon and choose **Workflows** > **Create Fabric Site**.

Step 3 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 4 In the **Fabric Site Location** window, choose an area, building, or floor to add as a fabric site.

Step 5 In the **Wired Endpoint Data Collection** window, ensure that the **Wired Endpoint Data Collection** check box is checked.

Step 6 In the **Authentication Template** window, do these tasks:

a) Choose an authentication template for the fabric site:

- **Closed Authentication**: Any traffic before authentication is dropped, including DHCP, DNS, and ARP.
- **Open Authentication**: A host is allowed network access without having to go through 802.1X authentication.
- **Low Impact**: Security is added by applying an ACL to the switch port, to allow limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.
- **None**

b) (Optional) If you choose **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:

- **First Authentication Method**: Choose **802.1x** or **MAC Authentication Bypass (MAB)**
- **802.1x Timeout (in seconds)**: Use the slider to specify the 802.1x timeout, in seconds.
- **Wake on LAN**: Choose **Yes** or **No**.
- **Number of Hosts**: Choose **Unlimited** or **Single**.

- **BPDU Guard**: Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
- **Pre-Authentication Access Control List**: Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

Step 7 In the **Fabric Zones** window, to designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now**.

To enable a fabric zone, choose a fabric site in the network hierarchy.

Step 8 In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Step 11 It takes a few seconds for the site and zones to be provisioned. A success message displays to confirm the creation.

The newly created fabric zone is tagged with an “FZ” in the site hierarchy pane.

Create a fabric zone within a fabric site

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 For the fabric site where you want to designate the fabric zone, under the **Actions** column, hover your cursor over the ellipsis icon (•••) and choose **Edit Fabric Zone**.

Step 4 In the **Edit Fabric Zones** window, choose an area, building, or floor.

Step 5 Review the fabric site settings in the **Summary** window.

You can edit any of the fabric site or zone settings here.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Step 8 It takes several seconds for the fabric site and fabric zones to provision. A success message displays to confirm the provisioning.

The newly created fabric zone gets an “FZ” in the site hierarchy pane.

What to do next

- Add only edge node and extended node devices to the newly created fabric zone.

  You can't assign to the parent site devices that are assigned to a fabric zone. However, you can configure an edge node device assignment to a fabric zone as a control plane or a border node for the parent site.

- Assign IP pools and virtual networks to the fabric zone.

Associate Layer 3 virtual networks to fabric zones

Before you begin

Ensure that you have created the fabric zone.

Note You can add only the Layer 3 virtual networks of a parent site to a fabric zone.

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Layer 3 Virtual Networks**.

The resulting window displays all the Layer 3 virtual networks at a global level.

Step 3 In the **Layer 3** tab, check the check box next to the Layer 3 virtual networks for which you want to edit the fabric zone associations.

Note You can edit up to five Layer 3 virtual networks.

Step 4 Hover your cursor over **More actions**, and choose **Edit Fabric Site and Fabric Zone Associations**.

Step 5 In the **Fabric Sites and Fabric Zones (Optional)** window, do this configuration:

a) Click **Select Fabric Zones** and choose the fabric zones.

You can assign a virtual network to multiple fabric zones in a fabric site. To choose the fabric zones, do one of these tasks:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.
c) Repeat this association for all the Layer 3 virtual networks.

Step 6 Review the Layer 3 virtual network zones on the **Summary** window.

Step 7 In the **Created and Deploy (Step 1 of 2)** window, click **Update**.

Step 8 In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to deploy the Layer 3 virtual networks.

Step 9 To verify the virtual networks, click **View Layer 3 Virtual Networks**.

In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

Associate Layer 2 virtual networks to fabric zones

Before you begin

Note After you add the gateways to a fabric zone, you can't edit them at the parent site.

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Layer 2 Virtual Networks**.

The resulting window displays all the Layer 2 virtual networks at a global level.

Step 3 Click Fabric Site: **Global**.

Step 4 In the **Select Fabric Site** slide-in pane, choose a fabric site and click **Select**.

Step 5 In the **Layer 2** tab, check the check box next to the Layer 2 virtual networks for which you want to edit the fabric zone associations.

Note You can edit up to five Layer 2 virtual networks.

Step 6 Hover your cursor over **More actions**, and choose **Edit Layer 2 Fabric Zone Associations**.

Step 7 In the **Associated Fabric Sites and Fabric Zones** window, do this configuration:

a) Click **Select Fabric Zones** and choose the fabric zones.

You can assign a virtual network to multiple fabric zones in a fabric site. To choose the fabric zones, do one of these tasks:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

c) Repeat this association for all the Layer 2 virtual networks.

Step 8 In the **Summary** window, review your Layer 2 virtual network settings and click **Create**.

Step 9 In the **Create** window, click **Deploy** to deploy the Layer 2 virtual network.

After the Layer 2 virtual network is provisioned, a success message is displayed.

Step 10 To verify the virtual network creation, click **View Layer 2 Virtual Networks**. In the **Virtual Networks** window, the **Layer 2** tab displays the details of all the Layer 2 virtual networks.

Associate anycast gateways to fabric zones

Before you begin

Ensure that you have created the fabric zone.

Note You can add only the anycast gateways of a parent site to a fabric zone.

After you add an anycast gateway to a fabric zone, you can't update it at the parent site.

Procedure

Step 1 From the main menu, choose **Provision** > **Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Anycast Gateways**.

The resulting window displays all the anycast gateways at a global level.

Step 3 Click Fabric Site: **Global**.

Step 4 In the **Select Fabric Site** slide-in pane, choose a fabric site and click **Select**.

Step 5 In the **Anycast Gateway** tab, check the check box next to the anycast gateways for which you want to edit the fabric zone associations.

Note You can edit up to five anycast gateways.

Step 6 Hover your cursor over **More actions**, and choose **Edit Fabric Zone Associations**.

Step 7 In the **Fabric Zones (Optional)** window, do these steps:

a) Click **Select Fabric Zones** and do one of these tasks:

- Click the plus icon next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Step 8 Review the anycast gateway settings in the **Summary** window.

Step 9 In the **Create** window, click **Deploy**.

Step 10 To verify the gateway creation after you see a success message, click **View Anycast Gateway**.

In the **Virtual Networks** window, the **Anycast Gateway** tab displays the details of all the anycast gateways.

Configure an extended node device

An extended node configures by automated workflow. After configuration, the extended node device displays in the fabric topology view. You can assign ports for the extended nodes using the **Port Assignment** tab.

Note You can't onboard the extended nodes through the GUI-based provisioning workflows. An extended node is onboarded only through the SD-Access automated workflow after resetting the device configuration to the factory default and powering on the device.

A device is onboarded according to the license of its extended node neighbor and its own license:

- If the neighbor is operating with an Essentials license, the device is onboarded as a standard extended node, regardless of its license.
- If the neighbor is operating with an Advantage license, the device is onboarded as a standard extended node if it has an Essentials license.
- If the neighbor is operating with an Advantage license, the device is onboarded as a policy extended node if it has an Advantage license.
- If the device has more than one neighbor, and those neighbors have different license levels, the device is onboarded as a standard extended node, regardless of its license.

Extended node devices support multicast traffic.

Policy-extended nodes are extended nodes that support security policy within the virtual network. You can choose a **Group** during port assignment for a policy-extended node.

Policy extended node devices include Cisco Catalyst Industrial Ethernet (IE) 3400, IE 3400 Heavy Duty series switches, and Cisco Catalyst 9000 series switches that run Cisco IOS XE Release 17.1.1s or later and Cisco Catalyst IE 3500 series switches running on Cisco IOS XE Release 17.18.x.

Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches, and Cisco Industrial Ethernet 4000, 4010, and 5000 series switches can't be configured as Policy Extended Nodes.

Configure an extended node

When configured as a fabric edge, Cisco Catalyst 9300, Cisco Catalyst 9400, and Cisco Catalyst 9500 Series switches support extended nodes.

Note Cisco Catalyst 9200 Series switches that are configured as fabric edge nodes don't support extended node devices.

The minimum supported software versions on the extended nodes include:

- Cisco Industrial Ethernet 4000, 4010, 5000 series switches: 15.2(7)E0s with LAN base license enabled.

  If you have an IP services license, you must change the Switch Database Management (SDM) template to `dual-ipv4-and-ipv6 default` manually.
- Cisco Catalyst IE 3400, 3400 Heavy Duty (X-coded and D-coded) series switches: Cisco IOS XE Release 17.1.1s.
- Cisco Catalyst IE 3500 series switches: Cisco IOS XE Release 17.18.x.
- Cisco Catalyst IE 3100, 3200 series switches: Cisco IOS XE Release 17.15.x.

- Cisco Catalyst IE 3300 series switches can operate as extended node when running the Essentials license: Cisco IOS XE Release 16.12.1s.
- Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches: Release 15.2(7)E0s.

The minimum software version that is required on a policy extended node device and on the edge node device supporting the policy extended node is Cisco IOS XE Release 17.1.1s.

This configuration steps are applicable to both a standard extended node and policy-extended node.

Before you begin

To configure a device as a policy-extended node, both the device and the edge node supporting it must have the Network Advantage license and Advantage license levels enabled.

Procedure

Step 1 Configure a network range for the extended node. See Configure IP address pools, on page 337. This step comprises adding an IP address pool and reserving the IP pool at the site level. Ensure that the CLI and SNMP credentials are configured.

Step 2 Assign the extended IP address pool to INFRA_VN. See Create anycast gateways, on page 1044. Choose **Extended Node** as the **Pool Type**.

Catalyst Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.

Step 3 Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Catalyst Center.

Note For a detailed description of Option 43, see DHCP controller discovery, on page 590.

Step 4 Connect the extended node device to the fabric edge device. You can have multiple links from the extended node device to the fabric edge.

Step 5 Create a port channel on the fabric edge node that is connected to the extended node. For a subsequent extended node in a ring or daisy chain, create the port channel on the previous extended node it connects to.

Note Complete this step only if the global authentication mode for the fabric is **Open Authentication**, **Low Impact**, or **Closed Authentication**. If the fabric site is set to **None** authentication mode, the port channel is automatically created during the onboarding of the extended nodes using Plug and Play provisioning.

To create a port channel, complete these steps:

a) From the main menu, choose **Provision** > **Fabric Sites**.
b) In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
c) Click a fabric site.
d) In the **Port Assignment** tab, choose **More Actions** > **Create Port Channel**.

e) Complete these tasks:

- Choose the fabric device for which a port channel has to be created.
- Choose an **Extended Node** in the **Connected Device Type** drop-down list.
- Enter a description.
- Choose **Port Aggregation Protocol (PAgP Desirable)**.

  Starting with Cisco IOS XE Release 17.1.1s, IE 3300 and IE 3400 devices support PAgP.
- Select **On** for IE 3300 and IE 3400 devices if they are running versions earlier than Cisco IOS XE Release 17.1.1s.

Note Link Aggregation Control Protocol (LACP) doesn't work for extended node onboarding.

- Choose the ports to be bundled as a port channel.

f) Click **Done**.

This creates a port channel on the fabric edge node (or the extended node) to onboard an extended device.

Step 6 Power up the extended node device if it has no previous configuration. If the extended node device has configurations, reset the device configuration to factory default and reload it.

Catalyst Center adds the extended node device to the inventory and assigns the same site as the fabric edge. The extended node device is then added to the fabric, onboarded, and ready to be managed.

Note An extended node device is added to the fabric only if the device runs a software release that is compatible with the Catalyst Center release. If the device runs an incompatible software release, it will not be onboarded. For information about fabric device compatibility, see Cisco SD-Access Compatibility Matrix.

After the configuration is complete, the extended node appears in the fabric topology with a tag (X) to indicate that it is an extended node.

Upgrade an extended node to a policy-extended node

Cisco SD-Access automation onboards a policy-extended node-capable device with an Essentials license as an extended node. You can convert this extended node device to a policy-extended node by upgrading its license to Advantage.

In a daisy chain, you can't upgrade an extended node to a policy-extended node if its upstream device is an extended node.

In a ring, you can't upgrade an extended node to a policy-extended node if both its neighbors are extended nodes.

After you upgrade the node to policy-extended node, you can't reconfigure it as an extended node.

To convert an extended node to a policy-extended node, do these steps.

Before you begin

- Ensure that the extended node is already onboarded.
- Update the Smart Licensing credentials on Catalyst Center.

Procedure

Step 1 Change the license level on the device from Essentials to Advantage, using the Catalyst Center License Manager:

a) From the main menu, choose **Tools** > **License Manager**.
b) In the **Devices** tab, check the check box next to the device.
c) Choose **Actions** > **Change License** > **Change Cisco License**.
d) In the **Change Cisco License Level** window, click **Advantage**.
e) Choose a license type.

Click the required license type: **All**, **DNA**, or **CNS**

f) Click **Continue**.
g) Check the **Reboot device on update** check box to reboot the device when its license level updates.
h) (Optional) In the **Task Name** field, update the task name.
i) Choose a schedule for updating the license level.

- **Now**: Immediately update the license level and reboot the device.
- **Later**: Schedule the date and time, and define the time zone to update the license level and reboot the device.

j) Click **Confirm**.

Step 2 Wait for the node to become **Reachable** and get to the **Managed** state.

The **Provision** > **Inventory** window displays the reachability status of all the devices.

Step 3 If you see a **Netconf Connection Refused** error, resynchronize the device. Repeat the resynchronization process until the error no longer displays.

a) In the **Provision** > **Inventory** window, choose the device.
b) Choose **Actions** > **Inventory** > **Resync Device**.

Step 4 Upgrade to policy-extended node.

a) In the **Provision** > **Fabric Sites** window, choose the site in which the device is onboarded.
b) In the **Fabric Infrastructure** tab, click a device to edit its attributes.
c) In the **Fabric** tab, click the **Policy Extended Node** toggle button under **Extended Node Attributes**. Then click **Add**.
d) In the **Policy Extended Node Upgrade** dialog box, click **Upgrade**.
e) In the **EN to PEN Upgrade** slide-in pane, schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

f) On the **Tasks** window, monitor the task deployment.

Delete an extended node

This task describes the steps to delete an extended node, policy-extended node, and authenticated extended node.

Procedure

Step 1 Remove the extended node device from the fabric.

a) From the main menu, choose **Provision** > **Fabric Sites**.
b) In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
c) Choose the fabric site that contains the extended node device.
d) In the **Fabric Infrastructure** tab, click the extended node device.
e) In the slide-in pane, click **Remove From Fabric**.
f) Click **Add**.

Step 2 Delete the device from **Inventory**.

For steps to delete the device from inventory, see Delete a network device, on page 183.

Step 3 For a supplicant-based extended node device, delete the port assignment configuration in the fabric edge node or the FIAB.

Configure a REP ring topology for extended nodes and policy-extended nodes

The Resilient Ethernet Protocol (REP) ring provides a way to control network loops, handle link failures, and improve convergence time.

Unless explicitly stated, the term *extended node* also represents a policy-extended node.

Devices that can be configured in a REP ring include:

- Extended node:

  Cisco Industrial Ethernet (IE) 4000, 4010, 5000 series switches that operate Cisco IOS 15.2(7)E3 and later releases.

  Cisco Catalyst IE3100, 3200, 3300, 3500, and 9300 series switches that operate Cisco IOS XE 17.3.3 and later releases.

- Policy-extended node:

  Cisco Catalyst IE3400, IE3400H series switches that operate Cisco IOS XE 17.3.3 and later releases.

Limitations of a REP ring

- Multiple rings within a given REP ring and a ring of rings aren't supported.
- A node in a REP ring can have other nodes connected to it in a daisy chain manner. However, a node in a daisy chain can’t have a ring of nodes connected to it.
- A REP ring or a daisy chain can't be a mix of extended nodes and policy-extended nodes. A REP ring or a daisy chain must consist entirely of either extended nodes or policy-extended nodes.
- By default, a maximum of 18 devices can be onboarded in a single REP ring. To onboard more than 18 devices, increase the BPDU timer using **spanning-tree vlan** *infra VN VLAN* **max-age 40** command. Use the Catalyst Center templates to configure the command.
- If a device in the REP ring is unreachable, Catalyst Center cannot delete the REP ring.

Note In some rare instances, when the last two nodes of the ring try to onboard simultaneously, a port channel might not be created between these nodes. A port channel is established between the last two nodes of the ring when a REP ring is created.

Unless otherwise stated, these steps are applicable to both extended node and policy-extended node.

Before you begin

Ensure that you have onboarded the fabric edge nodes and extended nodes.

Identify the fabric edge node and its interfaces that end the REP ring.

Note The REP ring configuration procedure may disrupt the network traffic for a brief period.

Procedure

Step 1 From the main menu, choose **Workflows**. Then locate the **Configure REP Ring (Fabric)** card and click **Start**.

Alternatively, you can:

a. Navigate to the fabric site topology view.

b. Click the fabric edge node or the FIAB node on which you want to create the REP ring to view its details.

c. Click **REP Rings**, then click **Create REP Ring**.

Step 2 If a task overview window appears, click **Let's Do It** to start the workflow.

Step 3 In the **Select a fabric site** window, select a site that has both edge nodes and extended nodes. Then click **Next**.

Step 4 In the **Select a fabric edge node** window, choose a fabric edge node. Then click **Next**.

Step 5 In the **Select extended nodes connected to fabric edge** window, choose two extended nodes that connect to the fabric edge node:

a) Choose the first extended node, then click **Next**.

b) Choose the second extended node, then click **Next**.

Step 6 Complete these tasks in the **Review your REP Ring discovery selections** window:

a) Enter a name for the REP ring you are configuring.
b) Confirm that the fabric site and devices you selected are displayed.
c) If necessary, click the appropriate **Edit** link to make changes.

Step 7 Initiate REP ring configuration by clicking **Provision**.

You can see a detailed status of the configuration progress on the **REP Ring Configuration Status** window.

Step 8 The **REP Ring Summary** window displays the details of the REP ring that is created along with the discovered devices.

Step 9 After the creation of the REP ring, a success message displays.

To verify the creation of the REP ring, go to the fabric site window and click the fabric edge node.

In the slide-in window, under the **REP Ring** tab, you can see the list of all REP rings that exist on that edge node.

Click a REP ring name in the list to view its details, such as the devices present in the ring, ports of each device that connect to the ring, and so on.

View REP ring status

To view the status of the devices in an REP ring:

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.

Step 3 Click a fabric site.

Step 4 In the **Fabric Infrastructure** tab, click the fabric edge node or the fabric in a box (FIAB).

A slide-in pane displays the details of the fabric edge node or the FIAB that is selected.

Step 5 In the **REP Rings** tab, click **View** to see the **REP Ring Topology Status**.

The **REP Topology Status** section displays the current state of all the devices in the REP ring. The state, as displayed in the **Role** column, can be **Open**, **Fail**, or **Alt**.

Open indicates that the device link is up and that it is forwarding traffic.

Fail indicates that the device link is down.

Alt indicates that the device link is up, but the port cannot forward traffic.

Delete a REP ring

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Infrastructure** tab, click the fabric edge node that ends the REP ring.

A slide-in window displays the details of the fabric edge node selected.

Step 3 In the **REP Rings** tab, for the desired REP ring, click **Actions (…)** > **Delete**.

This deletes the REP ring.

Note If any device in the REP ring is unreachable, you cannot delete the ring. Use Catalyst Center to rediscover the REP ring so you can remove unreachable devices and then delete the ring.

Add a node to a REP ring

Before you begin

Make sure you add the device to Catalyst Center. For information on how to add a device, see Add or edit a device, on page 596.

Note The feature supports these platforms: Cisco IE 2000 Series Switches, Cisco Catalyst IE 3200 Rugged Series Switches, Cisco Catalyst IE 3300 Rugged Series Switches, Cisco Catalyst IE 3400 Rugged Series Switches, Cisco Catalyst IE 3400 Heavy Duty Series Switches, Cisco IE 4000 Series Switches, Cisco IE 4010 Series Switches, Cisco IE 5000 Series Switches, Cisco IE 9300 Series Switches, and Cisco Catalyst ESS3300 Embedded Series Switches.

Follow these steps to add a single node to an existing REP ring. Nodes must be added one at a time.

Procedure

Step 1 Onboard and claim the device using the Plug and Play workflow.

a) From the main menu, choose **Provision** > **Plug and Play**.

The **Plug and Play** window displays the onboarded device.

b) From the **Actions** drop-down list, click **Claim**.

c) In **Assign Site** window, click **Assign** to assign the device to the site in which you want to add the node and click **Next**.

d) To deploy the configuration to the device, click **Assign** and click **Next**.

Note Plug and Play provisioning automatically deploys a device onboarding template for the device type. For more information, see Plug and Play provisioning overview, on page 585.

e) In the **Provision Templates** window, click **Preview Configuration** to review the configuration and click **Claim**.
f) Click **Ok** and **Yes**.

A success message appears when you claim the device.

g) Click **Refresh**. The device onboarding process might take some time.

By default, the devices table refreshes every 30 seconds. Click the **Auto-Refresh** drop-down list and choose a refresh time.

The device moves to the **Provisioned** tab when the process is complete.

Step 2 Verify that the device is in a managed state in the inventory.

a) From the main menu, choose **Provision** > **Inventory**.
b) Click **Refresh** to update the device status. Wait until the device is in a managed state.

Step 3 Add the device to the REP ring.

a) From the main menu, choose **Provision** > **Fabric Sites**.
b) In the **Fabric Sites** tab, click the fabric site that contains the device.
c) In the **Fabric Infrastructure** tab, click an edge node in the REP ring.

A slide-in pane displays the details of the selected node.

d) In the **REP Rings** tab, for the desired REP ring, under the **Actions** column, click the ellipsis (**…**) and choose **Rediscover**.
The node insertion status is **Success** for successful addition of the device to the REP.
e) (Optional) In the **REP Rings** tab, click the REP link to view the steps executed. If any failure occurs, you can view the step at which the device insertion failed.

Rediscover the failed node insertion, if necessary.

Delete a node from a REP ring

This task describes the steps to delete one extended node or multiple extended nodes from a REP ring.

Note After the extended nodes are removed, the downsized REP ring should use the existing interfaces to create a link to the neighboring devices.

Before you begin

Ensure that the REP ring to which the node belongs is not incomplete.

Procedure

Step 1 Manually remove the extended node devices from the network.

Alternatively, if a device in a REP ring goes down, the **Fabric Infrastructure** window displays a notification.

Step 2 From the main menu, choose **Provision** > **Fabric Sites**.

Step 3 In the **Fabric Infrastructure** tab, click the fabric edge node that ends the REP ring.

A slide-in pane displays the details of the selected fabric edge node.

Step 4 In the **REP Rings** tab, for the desired REP ring, choose **Actions (…)** > **Rediscover**.

The extended node device is deleted from the REP ring and the REP ring displays updates.

Configure supplicant-based extended nodes

Supplicant-based extended nodes, also called Authenticated Extended Nodes (AENs), are extended node devices that receive an IEEE 802.1x (Dot1x) supplicant configuration and are onboarded into the SD-Access network only after a complete authentication and authorization. To onboard a supplicant-based extended node device, the authenticator port on the fabric edge must be configured with a Closed Authentication Template.

These platforms support supplicant-based extended node onboarding:

Fabric Edge or FIAB:

Cisco Catalyst 9000 Series – C9300, C9400, C9500, and C9500H switches that operate Cisco IOS XE 17.7.1 or later.

Supplicant-based extended node:

Cisco Catalyst 9000 Series – C9200, C9300, C9400, C9500, and C9500H switches that operate Cisco IOS XE 17.7.1 or later.

Steps to configure a supplicant-based extended node

Before you begin

- Configure Cisco ISE and ensure that it operates Release 3.1 or later. See Configure Cisco Identity Services Engine to onboard supplicant-based extended node, on page 1071.
- Add the fabric edge node or FIAB device to the fabric and ensure that it operates Cisco IOS XE 17.7.1 or later.
- Set the Path MTU appropriately for the path between the fabric edge node and Cisco ISE. We recommend a value of 9100.

Note The Path MTU is set for all the devices in the fabric during LAN automation or when the underlay is configured.

Procedure

Step 1 Configure AAA server settings in Catalyst Center.

a) Define Cisco ISE as the AAA server for device authentication in the **System** > **Settings** > **External Services** > **Authentication and Policy Servers** window.

For the complete procedure, see "Configure Authentication and Policy Servers" in the *Cisco Catalyst Center Administrator Guide*.

b) Add the Cisco ISE server to the global site. For information, see Add Cisco ISE or other AAA servers, on page 319.

Step 2 (Optional) Configure Catalyst Center to authorize the device before onboarding.

a) From the main menu, choose **System** > **Settings** > **Device Settings** > **PnP Device Authorization**.
b) Check the **Device Authorization** check box to enable authorization on the device.
c) Click **Save**.

Step 3 Configure the Catalyst Center appliance to manage your PKI certificates.

a) From the main menu, choose **System** > **Settings** > **Certificates** > **Certificate Authority**.
b) In the **Certificate Authority** window, click **Use Cisco DNA Center**.
c) In the **CA Management** tab, click **Download** to download the CA Certificate.
d) Add the certificate to the Cisco ISE Trusted Certificate Store. For more information, see the Cisco Identity Services Engine Administrator Guide.

If you use an external certificate, add that certificate to the Cisco ISE Trusted Certificate Store.

Step 4 Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Catalyst Center.

For a detailed description of Option 43, see DHCP controller discovery, on page 590.

Step 5 Enable **Closed Authentication** and disable Bridge Protocol Data Unit (BPDU) Guard on the fabric Site.

By default, selecting Closed Authentication pushes the BPDU Guard configuration on all the downlink access ports. When a remote switch like an extended node is connected, BPDU Guard pushes the port to error disabled mode. To disable BPDU Guard, uncheck the **Enable BPDU Guard** check box during the Closed Authentication configuration.

For more information, see Select Authentication Template.

Step 6 Assign an extended IP address pool to INFRA_VN, as described in Create anycast gateways, on page 1044.

In the **Create Anycast Gateways** workflow, choose **Extended Node** as the **Pool Type** and check the **Supplicant-Based Extended Node Onboarding** check box.

Catalyst Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.

Note Extended IP address pool is successfully assigned only if the fabric edge devices operate Cisco IOS XE 17.7.1 or later. If you upgraded from an earlier release of Catalyst Center, the supplicant-based extended node migration must be complete before configuring the extended IP address pool.

Step 7 Connect the extended node device to the fabric edge node or the FIAB.

After powering on, the extended node device is in **Pending Authorization** state if you chose to authorize the device before onboarding (Step 2). You can check the status of the device in the **Provision** > **Plug and Play** window.

Step 8 (Optional) Authorize the device.

Perform this step only if the device is in **Pending Authorization** state.

a) From the main menu, choose **Provision** > **Plug and Play**.
b) In the **Plug and Play** window, select the supplicant-based extended node device and choose **Actions** > **Authorize**.

The authorization process provisions the supplicant-based extended node device for completing a certificate-based EAP-TLS authentication with Cisco ISE. After authentication, Cisco ISE authorizes the supplicant-based extended node device for complete access. The supplicant-based extended node device is then fully onboarded into the SD-Access fabric.

After a supplicant-based extended node device is onboarded into the fabric, access to the fabric edge-supplicant port is only based on authentication status. If the device or the port goes down, the authentication session is cleared, and traffic is not allowed on the port. When the port comes up again, it goes through the IEEE 802.1x (Dot1x) authentication process to regain access to the SD-Access network.

Replace a faulty port

If the link between the authenticator (fabric edge or FIAB) port and the supplicant port goes down, you can replace the faulty port and configure a new port through the **Port Assignment** menu.

Procedure

Step 1 To replace the supplicant port:

a) Clear the configuration on the new supplicant port.
b) Copy the existing configuration from the current supplicant port to the new supplicant port to allow 802.1X authentication.

Step 2 To replace the authenticator ports:

a) Assign the supplicant port to the new interface of the authenticator. For information on port assignment, see Configure ports within the fabric site, on page 1036. Choose **Supplicant-Based Extended Node** as the **Connected Device Type**.
b) Clear the existing port assignment on the old interface of the authenticator.

Step 3 Disconnect the physical connection between the old ports of the authenticator and the supplicant. Connect a cable between the new ports of the authenticator and the supplicant. Bring this link up.

Step 4 After the link between the new ports of the authenticator and supplicant is up, do these steps:

a) Resynchronize the device information in Catalyst Center by performing an **Inventory** > **Resync Device** for both the authenticator and the supplicant. See Resynchronize device information, on page 182.
b) Assign the new supplicant port to the authenticator. For information on port assignment, see Configure ports within the fabric site, on page 1036. Choose **Authenticator Switch** as the **Connected Device Type**.
c) Clear the port assignment on the old supplicant port.

Configure Cisco Identity Services Engine to onboard supplicant-based extended node

This task describes how to profile an Supplicant-Based Extended Node (SBEN) device in Cisco Identity Services Engine (ISE). The steps listed below are part of the Cisco ISE configuration procedure. For more information, refer the *Cisco Identity Services Engine Administrator Guide*.

Before you begin

Download the CA certificate from Catalyst Center.

Procedure

Step 1 Import the CA certificate into Cisco ISE:

From the Cisco ISE home page, choose **Administration** > **System** > **Certificates** > **System Certificates** > **Import**. In the **Import** window, ensure that you check the **Trust for client authentication and Syslog** check box. For more information, see the "Import the Root Certificates to the Trusted Certificate Store" section in the *Cisco Identity Services Engine Administrator Guide*.

Step 2 Configure these authorization profiles with their RADIUS attributes:

From the Cisco ISE main menu, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Configure these profiles:

```
SBEN-DHCP:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_DHCP_ACL.in
```

```
SBEN_LIMITED_ACCESS_AUTHZ:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_MAB_ACL.in
cisco-av-pair = interface-template-name=SWITCH_SBEN_MAB_TEMPLATE
```

```
SBEN_FULL_ACCESS_AUTHZ :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

Macsec encrypted onboarding

```
SBEN_FULL_ACCESS :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

Step 3 Under **Common Tasks**, configure these settings for Macsec encrypted SBEN onboarding:

a) Enable **Reauthentication** timer option.

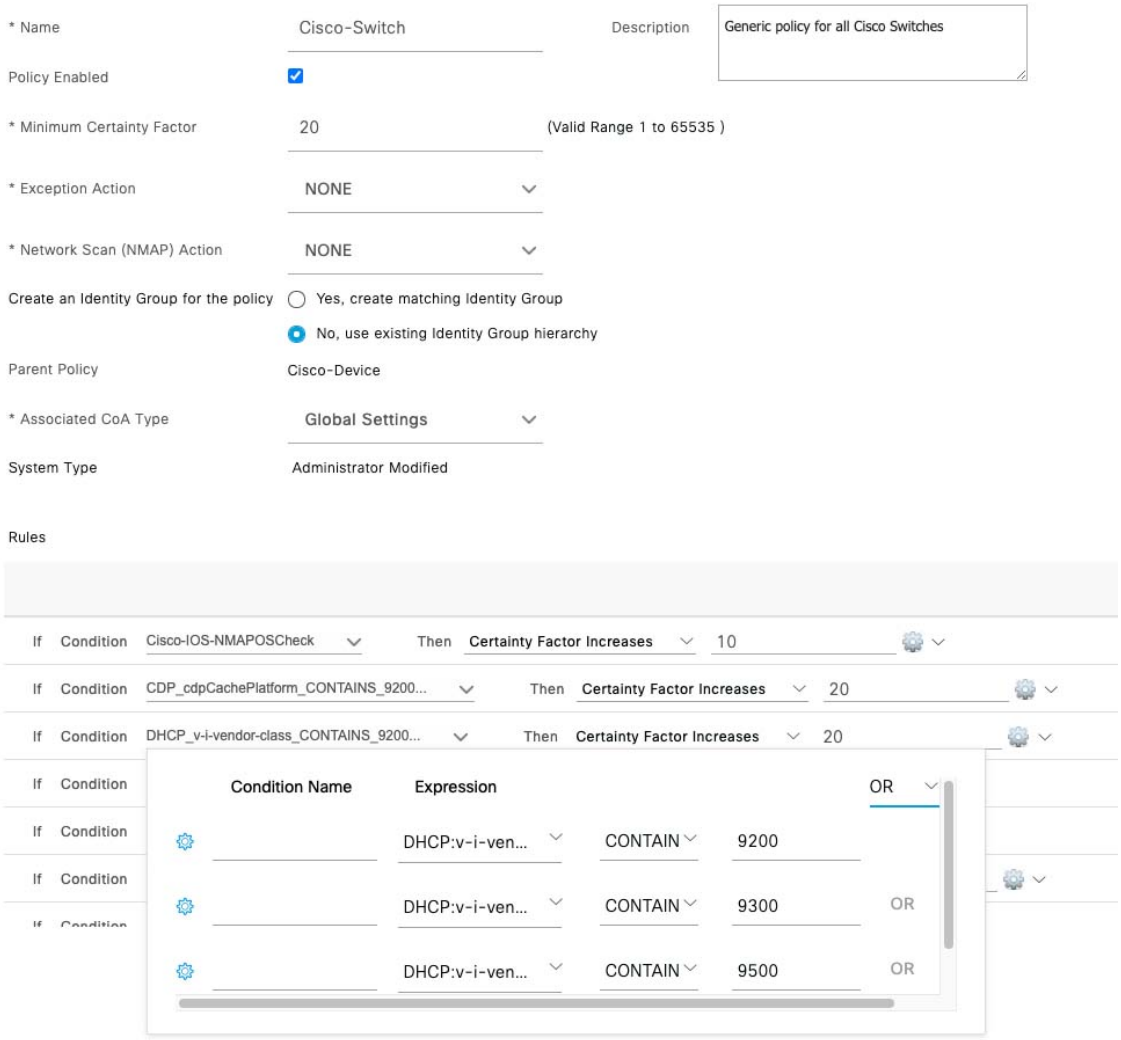
b) Enable **Macsec policy** option.

- Select the **should-secure** option during SBEN onboarding.
- Select the **must-secure** option after SBEN onboarding.

Step 4 Define the device profiling policy in the **Profiling Policies** window.

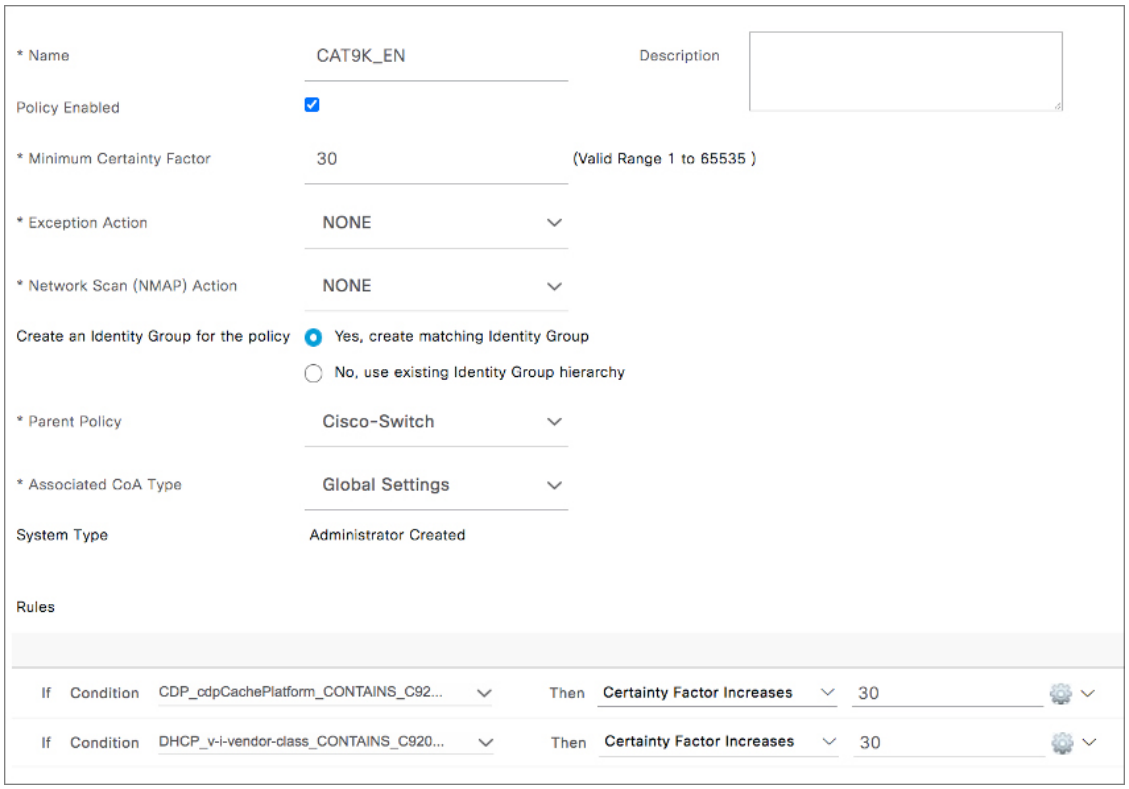
a) From the Cisco ISE main menu, choose **Policy** > **Profiling** > **Profiling Policies**.

b) In the **Profiling Policies** window, add a new **DHCP-v-i-vendor-class** condition for the **Cisco-Device**: **Cisco-Switch** policy.



c) Create a new child policy for the supplicant device, under **Cisco-Switch** and apply the **CdpCachePlatform** and **V-I-Vendor-Class** conditions.

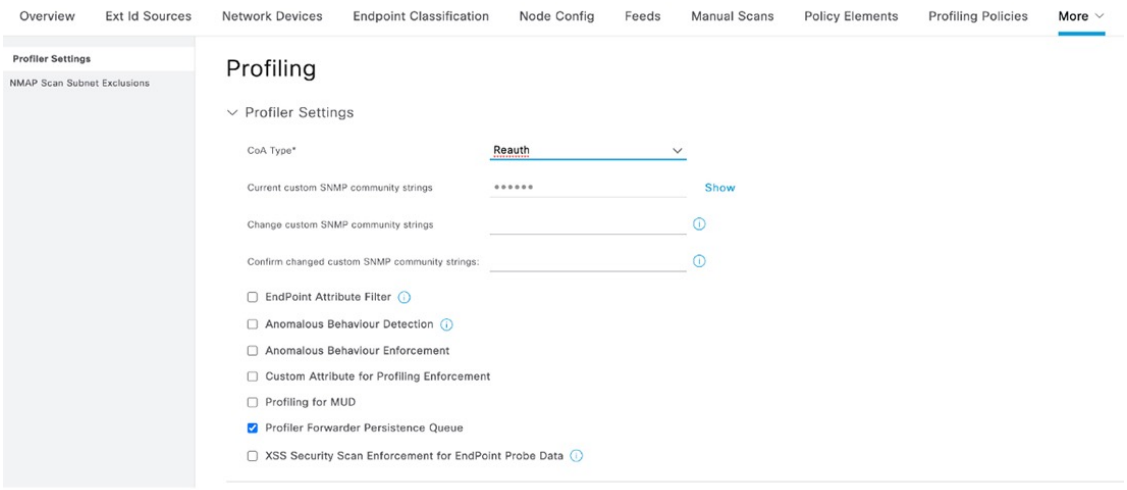
Ensure that the **Minimum Certainty Factor** value for the child policy is higher than that of the parent policy.



Step 5 Set the global Change of Authorization (CoA) type to **Reauth**.

To configure the **CoA Type**, from the Cisco ISE home page, navigate to **Work Centers** > **Profiler** > **Settings**.

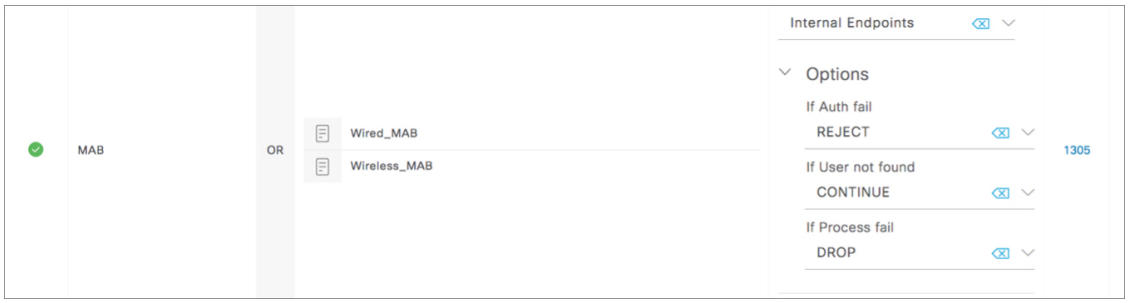
Choose **Reauth** from the **CoA Type** drop-down list.



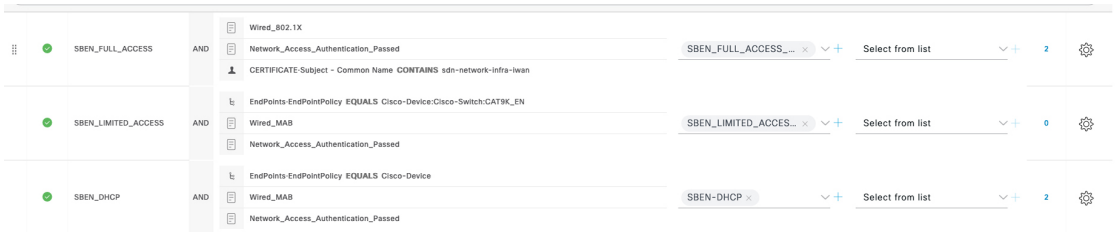
Step 6 Define the authorization policy in the **Authorization Policy** window.

a) From the Cisco ISE home page, choose **Policy** > **Policy Sets** > **Default** > **Authorization Policy**.

b) Ensure that the default MAB policy is set to **CONTINUE** option for the **If User not found** field.



c) In the **Authorization Policy** window, configure the authorization policies for the supplicant device and associate the policies with the authorization profiles that were created earlier (SBEN-DHCP, SBEN_LIMITED_ACCESS_AUTHZ, SBEN_FULL_ ACCESS_AUTHZ).



Configure a port channel

A group of ports bundled together to act as a single entity is called a port channel. Port channels between a fabric edge and its remotely connected devices, such as extended nodes or servers, increase the connection resiliency and bandwidth.

Create a port channel

Before you begin

The authentication must be **Closed Authentication**.

Note These steps are automated for other authentication modes.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, click a fabric site to configure port channels.

Step 4 In the **Port Assignment** tab, hover your cursor over **More Actions**, and click **Create Port Channel**.

Step 5 In the **Select your fabric devices** window, select the fabric devices for which a port channel has to be created.

Step 6 To specify the number of port channels and configure each port channel, do these tasks in the **Determine number of port channels** window:

a) From the **Connected Device Type** drop-down list, choose the type of connected device:

- To create a port channel between a fabric edge node and an extended node or between two extended nodes, choose **Extended Node**.
- To create a port channel with a fabric edge node or extended node on one side and a third-party device or a server port on the other side, choose **Trunk**.

  Configure **Native VLAN** and **Allowed VLANs** values for the trunk port.

  - In the **Native VLAN** field, enter a value for the native VLAN.

    The valid range is from 1 to 4094. The default value is 1.

  - In the **Allowed VLANs** field, you can choose to allow all VLANs, a specific VLAN ID between 1 and 4094, or specify a range of VLANs. For example, you can enter 100, 200, or 300-400. The default value is **All**.

Note When templates override default values, update the trunk configuration to align with the values that are specified for each port in the template.

b) Enter a **Description** for the new port channel.

c) Choose a protocol:

- For the extended nodes that run Cisco IOS XE Release 16.12.1s and earlier releases, choose **On** as the protocol.
- For the extended nodes that run Cisco IOS XE Release 17.1.1s and later releases, choose **Port Aggregation Protocol (PAgP)** as the protocol.
- Don't select **Link Aggregation Control Protocol (LACP)** as the protocol for extended nodes. You can only connect the trunk ports or the server ports in the LACP mode.

Step 7 From the list of available interfaces, choose the interfaces to be bundled as a port channel.

Note You cannot have more than 16 members in a port channel that is connected in the LACP mode.

You cannot have more than eight members in a port channel that is connected in the PAgP mode.

Step 8 In the **Summary** window, review the port channels that are created.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Update a port channel

Before you begin

Ensure that at least one member interface exists before you update a port channel.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, click a fabric site to update the port channels.

Step 4 In the **Port Assignment** tab, choose the port channel to be updated.

Step 5 Hover your cursor over **More Actions**, and click **Edit Port Channel**.

Step 6 Follow the onscreen guidelines to update the port channel configuration.

You can either add interfaces to the port channel or delete existing interfaces on the port channel.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Delete a port channel

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Click a fabric site.

Step 4 In the **Port Assignment** tab, choose the port channel to be deleted.

Step 5 Hover your cursor over **More Actions**, and click **Delete Port Channel**.

Step 6 At the prompt, click **Yes**.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Multicast

Multicast traffic is forwarded in different ways:

- Through shared trees by using a rendezvous point. PIM SM is used in this case.
- Through shortest path trees (SPT). PIM source-specific multicast (SSM) uses only SPT. PIM SM switches to SPT after the source is known on the edge router that the receiver is connected to.

See IP Multicast Technology Overview.

Configure multicast

Catalyst Center provides a workflow to enable group communication or multicast traffic in virtual networks. The workflow also allows you to choose multicast implementation in the network: native multicast or headend replication.

Note You can enable multicast on a virtual network whose border serves as a multisite remote border. Configuring multicast on such a virtual network configures multicast on the devices in the inherited virtual network too, provided the inherited virtual network already contains a segment. If the inherited virtual network doesn't have a segment, multicast is deployed only after the first segment is created. Ensure that a virtual network and its inherited networks deploy the same type of multicast implementation. The edge node devices of an inherited virtual network cannot be configured as a rendezvous point (RP).

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure Multicast**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Fabric Site** window, select a site in the site hierarchy pane.

Step 4 In the **Replication Mode** window, choose the method of multicast implementation for the network from these locations:

- **Native Multicast**
- **Head-end replication**

Step 5 In the **Virtual Networks** window, choose the virtual network for which you want to set up multicast.



Note You can't select an inherited virtual network to set up multicast.

Step 6 In the **Multicast pool mapping** window, select an IP address pool from the **IP Pools** drop-down list. The selected IP address pool is associated with the chosen virtual network.

Step 7 In the **Multicast Mode** window, choose the type of multicast to implement:

- **SSM** (Source Specific Multicast)
- **ASM** (Any Specific Multicast)
- Select **SSM** and **ASM** to configure both together.

Step 8 Do these steps:

a) On selecting **SSM**, configure the SSM list by adding an IP group range for each virtual network. You can add multiple IP group ranges for a virtual network.

1. By default, 232.0.0.0/8 range of IPv4 address is selected. You can optionally modify the IPv4 address range.

   Choose an IP group range from 225.0.0.0 to 239.255.255.255.

2. For IPv6 addresses, FF3x::/32 is reserved for SSM.

b) On selecting **ASM**, in the **Multicast Group to Rendezvous Point Mapping** window, configure the rendezvous point for each virtual network:

1. Choose the type of rendezvous point: **External** or **Fabric**.
2. Configure the rendezvous points in the respective tabs: **IPv4 RP** and **IPv6 RP**.
3. You can define any number of external rendezvous points.
4. Optionally, you can define a group-to-rendezvous point mapping. There could be one or multiple IPv4/IPv6 multicast groups that are associated with a rendezvous point.
5. You can either have a rendezvous point with no mapping or with mapping. Both can't be configured together.
6. The permitted multicast group ranges for IPv6 and IPv4 FF00:/8 and 225.0.0.0/8 - 239.0.0.0/8 respectively.

Step 9 In the **Summary** window, review the multicast settings. To modify any of the settings, click **Edit**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 On the **Tasks** window, monitor the task deployment.

Edit BGP AS number for a fabric site

Use this procedure to edit the BGP Autonomous System (AS) number for a fabric site.

Changing the BGP AS Number temporarily disrupts BGP peerings and removes any custom BGP configurations on border nodes and control plane nodes, requiring updates to templates and reconfiguration of custom settings. BGP AS number change can cause a temporary outage of external connectivity for all virtual networks and potentially disrupt management access.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 In the **Fabric Sites** window, select the fabric site for which you want to edit the BGP AS number.

Step 4 In the corresponding fabric site window, hover your cursor over **Site Actions** and choose **Edit BGP AS Number**.

Step 5 Review the information in the **Edit BGP AS Number** dialog box and click **Edit**.

Step 6 In the **New Local BGP AS Number** field, enter the new BGP AS number.

The valid range is 1 to 4294967295.

Step 7 Click **Deploy**.



Important Ensure that the device is reachable for successful deployment.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

What to do next

If you have configured BGP customizations using CLI templates, update the AS number in the corresponding CLI templates before reapplying them.

Shared wireless controllers for multiple fabric sites

A shared wireless controller is a single Cisco Catalyst 9800 Series Wireless Controller that is associated with more than one SD-Access fabric site. Use this deployment when multiple nearby physical locations are deployed as separate fabric sites and the same wireless controller must manage APs across those sites.

Each site maintains independent address pools and control-plane nodes, which ensures logical and network isolation across sites. This setup simplifies wireless network management and reduces hardware requirements.

A shared wireless controller architecture for multiple fabric sites is a deployment model that

- enables a single wireless controller to manage APs across multiple fabric sites,
- maintains site autonomy so each site keeps independent client address pools, control-plane nodes, and Layer 2 domains, and
- reduces hardware footprint and ensures policy consistency without consolidating participating fabric sites into a single logical site.

The deployment requires low latency, defined as round-trip time of 20 ms or less, between APs and the shared wireless controller. It limits sharing to up to 16 fabric sites based on control-plane-name constraints. All participating sites must use the same network underlay type. Each site allocates unique IP address pools for APs. Site-specific configuration differences, such as SSIDs, network profiles, or VLAN names, are resolved using Catalyst Center workflows before wireless controller sharing is enabled.

Do not use this feature for sites that are separated by a WAN.



Note This feature is in beta.

This deployment includes site-specific roles and terminology that support network segmentation and operational independence.

- Local site: The original fabric site where the wireless controller is first provisioned.
- Remote site: Any fabric site, other than the local site, where the shared wireless controller manages APs.
- Shared site: Any fabric site (local or remote) where the wireless controller operates and manages APs.

After the wireless controller is shared, the local site remains the fixed home site.

Requirements and guidelines

Review these requirements before you share a wireless controller across fabric sites:

- The wireless controller must be added to its local fabric site before it can be shared with a remote fabric site.
- Each remote fabric site must be selected during wireless controller reprovisioning before the wireless controller can be added to that remote fabric site. A wireless controller can participate in up to 16 fabric sites. Each site supports up to two map servers when hosting a shared wireless controller.
- Each selected remote fabric site must have at least one managed AP location, primary or secondary, within that fabric-site hierarchy.

- Each remote fabric site must have the required fabric roles for wireless fabric operation, including a control plane and map server.
- All fabric sites that share the same wireless controller must use the same underlay type.
- Catalyst Center can reuse an existing network profile when it is compatible with every selected site. If sites that share a network profile require different site-specific wireless settings, Catalyst Center creates a site-specific copy of the existing profile for the newly shared site. The existing profile remains unchanged.
- Sites can use the same SSID or WLAN name when the wireless settings are compatible. Policy profile names, fabric profile names, custom policy tag mappings, Layer 2 virtual network identifiers, and wireless-pool VLAN names must not conflict across fabric sites that share the same wireless controller.



Note Catalyst Center handles Layer 2 virtual network identifier conflicts automatically. When you add the shared wireless controller to a remote fabric site, Catalyst Center can assign new Layer 2 virtual network identifier values to ensure that the values are unique across all fabric sites that share the wireless controller. Catalyst Center then updates the affected fabric devices to use the new values. This update can temporarily interrupt traffic in affected segments.

- Each fabric site must use a different IP address pool. Reusing the same IP address pool across fabric sites is not supported. Client IP address pools can be different or reused across the sites.
- This feature is supported only for the wireless controllers that are onboarded on a fabric site. Wireless controllers that are onboarded on a nonfabric site do not support this feature.

  Supported platforms include Catalyst 9800 Series Wireless ControllerCisco Catalyst 9800 Series Wireless Controllers (C9800-40, C9800-80, C9800-L, C9800-CL, CW9800M, CW9800H1, CW9800H2, CW9800H3, CW9800L).



Note Cisco AireOS Wireless Controllers, embedded wireless controllers, and wireless modes like OfficeExtend Access Point (OEAP) are not supported.

Validation checks

Catalyst Center performs these validation checks:

- Wireless controller platform compatibility
- Controller provisioning to its local site before sharing
- Site independence and role configuration (presence of map server and control-plane node)
- Conflict-free network profiles, SSID settings, wireless mappings, IP address pools, and VLAN names
- Scale limits on control-plane-name and map-server roles not exceeded
- User authorization across all sites to make configuration changes

Traffic impact

Adding a wireless controller to a remote fabric site or removing it from a fabric site can temporarily interrupt traffic in affected segments. If both wired and wireless connectivity are enabled in an affected segments, traffic for both wired and wireless clients in that subnet can be interrupted. Perform these changes during a maintenance window.

Site-based, role-based access control

Shared wireless controller operations can affect more than one fabric site. Catalyst Center evaluates authorization according to the site scope, target device, and the requested operation.

To perform inventory provisioning or fabric operations on a shared wireless controller, or on another device in a site containing a shared wireless controller, you must have access to all fabric sites associated with the shared wireless controllers in that site. View access can differ from configuration access.

These tables show the permissions for wireless controllers and switches based on the site access.

Table 53: Wireless controller authorization

User scope	Wireless controller context	View	Inventory provisioning and fabric operations
Site-scoped user	Dedicated wireless controller in a site containing only dedicated devices	Yes	Yes
Site-scoped user	Dedicated wireless controller in a site containing a shared wireless controller	No	No
Access to all associated shared sites	Shared wireless controller	Yes	Yes
Access does not include all associated shared sites	Shared wireless controller	No	No

Table 54: Switch authorization

User scope	Switch context	View	Inventory provisioning and fabric operations
Site-scoped user	Switch in a site containing only dedicated devices	Yes	Yes
Site-scoped user	Switch in a site containing a shared wireless controller	No	No
Access to all associated shared sites	Switch in a site containing a shared wireless controller	Yes	Yes

User scope	Switch context	View	Inventory provisioning and fabric operations
Access does not include all associated shared sites	Switch in a site containing a shared wireless controller	Yes	No

Configure a shared wireless controller for multiple fabric sites

Use this procedure as an overview of the tasks required to share a wireless controller across multiple fabric sites.

Before you begin

Review traffic impact when you share a wireless controller, schedule the change for a maintenance window, and confirm that you have access to the local site and all remote sites.

Procedure

Step 1 Complete these readiness check:

a) Identify the local fabric site and each remote fabric site, and confirm that the wireless controller model supports this deployment.

b) For each remote site, confirm that the wireless controller manages at least one AP location and that the site has the required control plane and map server roles.

c) Confirm that all participating sites use the same underlay type, each site uses a different IP address pool, and the AP to wireless controller round-trip time is 20 ms or less.

d) Confirm that the deployment does not exceed 16 fabric sites and that you have access to the local site and every remote site.

For more information, refer to Shared wireless controllers for multiple fabric sites, on page 1080.

Step 2 Prepare network profiles for wireless controller sharing to review SSID settings and site-specific wireless objects. For more information, refer to Prepare network profiles for wireless controller sharing, on page 1084.

Create a site-specific copy of a shared network profile only when the participating sites require different settings.

Step 3 Provision the wireless controller and add it to the local fabric site. For more information, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 4 Reprovision the wireless controller with these configurations for sharing the wireless controller:

a) Configure the remote fabric sites as managed AP locations.

b) Check the **Share With Fabric Sites** check box, and select the remote fabric sites.

c) In the **Edit Fabric Sites** slide-in pane, ensure that the **Split Network Profiles for new shared Fabric Sites** option is selected when Catalyst Center must create a site-specific copy of an existing network profile for a newly shared site.

d) Resolve the conflicts.

For more information, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 5 Add the shared wireless controller to each remote fabric site, one site at a time. For more information, refer to Add a shared wireless controller to a remote fabric site, on page 1085.

Step 6 Configure the wireless SSIDs, IP address pools, security groups, and any required wireless multicast settings for each fabric site. For more information, refer to Configure wireless SSIDs for fabric networks, on page 1038.

Step 7 Provision the APs in each remote fabric site. For more information, refer to Provision Cisco APs on day 1, on page 627.

Step 8 Review the local and remote fabric sites.

a) From the main menu, choose **Provision** > **Fabric Sites**.

b) Choose the fabric site.

The resulting topology view displays all devices in the network.

c) In the **Fabric Infrastructure** tab, hover your cursor over the wireless controller, under **Current Shared Fabric Sites** confirm that the local site and each required remote site are listed.

Step 9 Verify that the APs and wireless clients are healthy.

a) From the main menu, choose **Assurance** > **Health**.

b) From the site hierarchy, select the remote fabric site.

c) In the **Overall** tab, review **Network Devices** and **Wireless Clients**.

d) Click **View Client Health** to open the **Client Health** dashboard and confirm that the wireless client is active and healthy.

For information about monitoring the overall health, see "Monitor and Troubleshoot Overall Enterprise Health" in the *Cisco Catalyst Assurance User Guide*.

Prepare network profiles for wireless controller sharing

Use this procedure to prepare network profiles for sharing a wireless controller across multiple fabric sites.

Review the wireless design for every participating site. Catalyst Center reuses a compatible site-specific network profile. When sites share a network profile and require different site-specific settings, Catalyst Center creates a copy for the remote site and creates or updates the corresponding policy profiles.

Note Catalyst Center separates a profile only when the newly added site requires different site-specific settings. The existing network profile for the local site remains unchanged. Catalyst Center does not change site-level overrides automatically.

Before you begin

- Identify the local fabric site and each remote fabric site that will share the wireless controller.
- Make sure that each remote fabric site has at least one managed AP location.
- Make sure that each participating site has the required wireless profile, SSIDs, virtual networks, and IP address pools.

Procedure

Step 1 Open the network profile used by the site that you plan to add.

For more information, refer to Create network profiles for wireless, on page 460.

Step 2 Review the sites, wireless SSIDs, WLAN profile names, and policy profile names in the network profile.

Step 3 Configure any custom policy tags, CLI templates, and feature templates associated with the profile.

Note The conflict resolution does not clone these configurations during the wireless controller provisioning.

Step 4 Make sure that wireless pool VLAN names are unique across the fabric sites that will share the wireless controller.

Step 5 Save any required network profile changes.

What to do next

Provision the wireless controller and select the remote fabric sites. If Catalyst Center detects a conflict for a newly added site, resolve it in **Edit Fabric Sites** slide-in pane. For more information, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Add a shared wireless controller to a remote fabric site

Use this procedure to add the shared wireless controller to a remote fabric site. Add the shared wireless controller to a single remote fabric site at a time.

Before you begin

- Ensure that the wireless controller manages at least one AP location in the remote fabric site hierarchy. For more information, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.
- Ensure that you select the fabric site using the **Share With Fabric Sites** option and reprovision the wireless controller. For more information, refer to Configure a shared wireless controller for multiple fabric sites, on page 1083.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Choose the remote fabric site.

The resulting topology view displays all devices in the network.

Step 3 In the **Fabric Infrastructure** tab, click the wireless controller name.

Step 4 In the slide-in pane, complete these configurations:

a) Under the **Fabric** tab, enable the **Wireless LAN Controller** toggle button.

b) Click **Add**.

Step 5 Click **Deploy**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.

- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Edit remote fabric sites for a shared wireless controller

Use this procedure as an overview of the tasks required to add or remove remote fabric sites for a shared wireless controller.

Procedure

Step 1 To remove a remote fabric site from a shared wireless controller, remove the shared wireless controller from fabric in the remote site.

For more information, refer to Remove a shared wireless controller from a fabric, on page 1086.

Step 2 Reprovision the shared wireless controller with these configurations:

a) (Optional) Configure any new remote fabric sites as managed AP locations.
b) In **Share With Fabric Sites**, click **Edit**, and add or remove remote fabric sites.
c) In the **Edit Fabric Sites** slide-in pane, ensure that the **Split Network Profiles for new shared Fabric Sites** option is selected when Catalyst Center must create site-specific copies of network profile for the newly shared sites.
d) Resolve the conflicts, review the configuration preview, and deploy the wireless controller configuration.
e) If the managed AP locations change after site selection, Catalyst Center displays a warning message. Review the site selection before provisioning.

For more information, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 3 If you added new remote fabric sites, add the shared wireless controller to each newly added remote fabric site, one site at a time. For more information, refer to Add a shared wireless controller to a remote fabric site, on page 1085.

Remove a shared wireless controller from a fabric

Use this procedure to remove a shared wireless controller from a remote fabric site or the local fabric site.

Before you begin

Review the traffic impact and plan the change for a maintenance window.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Choose the fabric site.

The resulting topology view displays all devices in the network.

Step 3 In the **Fabric Infrastructure** tab, click the wireless controller name.

Step 4 In the slide-in pane, complete these configurations:

a) Under the **Fabric** tab, click **Remove From Fabric**.

b) Click **Add**.

Step 5 Click **Deploy**.

Step 6 Schedule the task for deployment.

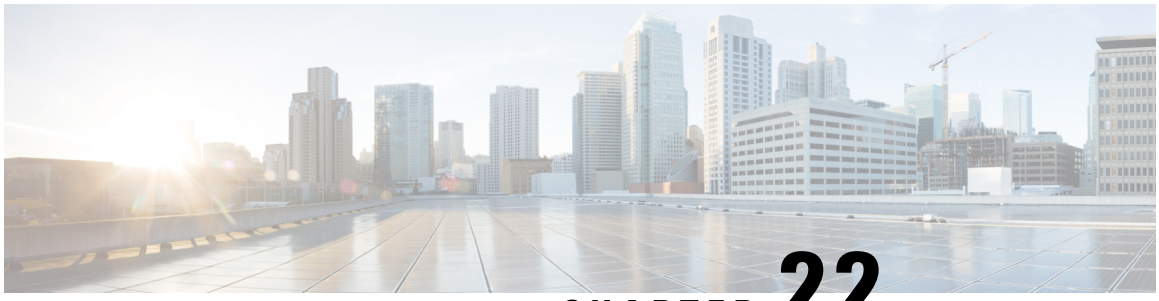
Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Step 8 If a remote fabric site no longer needs to share the wireless controller, remove that site from the **Edit Fabric Sites** slide-in pane and reprovision the wireless controller. For more information, refer to Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 9 (Optional) To remove the wireless controller from its local fabric site, repeat Step 2, on page 1086 to Step 7, on page 1087 to remove it from all remote fabric sites.



CHAPTER 22

Provision Campus Networks

- Campus networks, on page 1089
- Manage networks, on page 1090
- Manage configuration profiles, on page 1092
- Manage switching device groups, on page 1099
- Manage devices, on page 1105
- Compare device configurations, on page 1111

Campus networks

The Campus Network feature allows you to manage and standardize configurations across campus environments for Cisco Catalyst Switches (Cisco Catalyst 9000 Series Switches and Cisco Catalyst Industrial Ethernet (IE) Switches) and Cisco Catalyst 9800 Series Wireless Controllers. This feature helps you keep configurations consistent and scale your deployments across multiple sites.

In a campus network, networks act as logical containers for managed devices. To support configuration consistency, Catalyst Center uses configuration profiles. You can use these profiles to deploy consistent and standardized configurations on other devices. You can compare a device configuration with a configuration profile to identify deviations.

Note This feature is in beta.

Switches

Catalyst Center supports creation of switching device groups, which are a collection of devices intended to have similar configurations. A network can include one or more device groups as well as individually managed devices, providing flexibility in switch deployment and management across sites. You can create new configuration profiles for switches or learn the device configurations from an existing device.

Wireless controllers

Catalyst Center can create new configuration profiles for wireless controllers or learn configurations from an existing wireless controller and save them as configuration profiles.

For more information about campus networks configuration for wireless controllers, refer to Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers, on page 1450.

Manage networks

Use this procedure to view and manage networks in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

If there are no existing networks, use the **Create Network** option to create a new network. For more information, see Create a network, on page 1091.

For existing networks, the list of networks is displayed with details, such as the number of device groups and devices and the site associated with the network.

To...	Do this...
Edit or delete a network	Hover your cursor over the ellipsis icon and choose **Edit network name** or **Delete network**, as required. You cannot delete a network that has a device group attached to it.
Add a network	Click **Create Network**. See Create a network, on page 1091.
View network details	Click a network. See the next step.

Step 2 Click a network to view details of the network.

The window displays these details:

Name	Description
Device groups	This tab displays all the device groups associated with the network with details like the type of the device group and number of devices in the device group. **Switching device groups**: Click **Create switching device group** to add a new switching device group. In the create window, enter a device group name, add devices (optional) and click the create option. Hover your cursor over the ellipsis icon and choose **Edit** or **Delete**, as required. You cannot delete a device group that has devices assigned to it. To view the device group details, click a device group name. For more information, see Manage switching device groups, on page 1099.

Name	Description
Devices	This tab displays the list of network devices associated with the network with details such as the IP address, manageability status, the device group it belongs to, and so on. To view the device details, click a device name. See Manage devices, on page 1105.

Create a network

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

This table describes what occurs based on the presence of existing networks.

If...	Then...
there are no existing networks	**Create Network** option is displayed.
there are existing networks	a list of the available networks is displayed with the **Create Network** option to add a new network.

Step 2 Click **Create Network**.

Step 3 In the **Create Network** window, configure these fields:

Network details

- **Network name**: Enter a name for the network.
- **Site**: Choose a site for the network. All devices that are associated with the site and the levels below it will be added to the network.

You can create a device group or add individual devices to your network. Choose from the available options.

Option	Action
Create a switch device group	Enter a **Device group name**. Optionally, add devices to your device group.
Add WLCs	Select wireless controllers to add to your network.
Do this later	Select to skip the device group creation.

Step 4 Click **Create Network**.

Manage configuration profiles

You can create configuration profiles or learn profiles from an existing device and assign these profiles to device groups and devices across the network. Use this procedure to add, edit, and delete configuration profiles.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Use this table to configure the configuration profiles.

Table 55: Switching profiles

To...	Do this...
Create a configuration profile	Click **Create new**. For more information, refer to Create a configuration profile for switching device group, on page 1093.
Learn profile from an existing device	Click **Learn from a switch**. For more information, refer to Learn configuration profiles from a switch, on page 1101.
Edit a profile	Click the profile name and make the necessary updates.
Delete a profile	Choose **Delete** under the **Actions** column.
Duplicate a profile	Choose **Duplicate** under the **Actions** column and enter a name for the configuration profile.

Table 56: Wireless profiles

To...	Do this...
Create profiles for a wireless controller	Click **Create new**. For more information, refer to Create configuration profiles for wireless controllers, on page 1096.
Learn profiles from a wireless controller	Click **Learn from a WLC**. For more information, refer to Learn configuration profiles from a wireless controller, on page 1097.
Edit a profile	Click the profile name and make the necessary updates.
Assign profile to wireless controllers	Under **Actions**, click **Assign** or click the corresponding ellipsis icon and choose **Assign to devices**. Select the devices and click **Assign**. You can view the number of devices the profile is assigned to in the Configuration profile window.
Unassign profile from wireless controllers	Under **Actions**, click the corresponding ellipsis icon and choose **Unassign from devices**. Select the devices and click **Unassign**.
Delete a profile	**a.** Under **Actions**, click the corresponding ellipsis icon and choose **Delete**. **b.** In the dialog box, click **Delete**.

To...	Do this...
Duplicate a profile	**a.** Under **Actions**, click the corresponding ellipsis icon and choose **Duplicate**. **b.** In the **Duplicate configuration profile** dialog box, enter a unique name for the configuration profile. **c.** Click **Duplicate**.

Create a configuration profile for switching device group

Use this procedure to create a configuration profile for switching device groups.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click **Configuration profiles**.

Step 3 In the **Switching** tab, choose the type of profile in the left pane and click **Create New**.

For port configuration profiles, refer to Create port configuration profiles for switching device groups, on page 1093.

For other supported profiles, follow the next steps.

Step 4 Enter a **Configuration profile name** and optionally, a **Configuration profile description**.

Step 5 Configure the profile attributes based on the type of configuration.

Refer to Manage per-device configurations for Cisco Catalyst Switches, on page 96 for information on the configurations.

Step 6 After configuring the required profile settings, click **Create configuration profile**.

Create port configuration profiles for switching device groups

Use this procedure to create port configuration profiles for switching device groups.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**

Step 2 Click **Configuration profiles**.

Step 3 In the **Switching** tab, select **Ports**.

Step 4 Click **Create new** and choose the port profile type.

Step 5 Use the table to configure the profile attributes.

Click **Add configurations** to add more configurations to the profile.

Profile type	Description
L2 port profile	• **Port Configuration Profile Name**: Enter a name for the profile. • **Port Configuration Profile Description**: Enter a description for the profile. • **Description**: Description of the interface. • **Admin Status**: Enable or disable the interface. • **Layer 3**: Enable or disable switchport mode on the interface. • **Port Mode**: Select the port mode from the drop-down list.
L3 port profile	• **Port Configuration Profile Name**: Enter a name for the profile. • **Port Configuration Profile Description**: Enter a description for the profile. • **Description**: Description of the interface. • **Admin Status**: Enable or disable the interface. • **Layer 3**: Enable or disable switchport mode on the interface. • **IPv6**: Enables IPv6 on the interface. **IPv4**: • **IP Address Type**: Choose the IP address type for the interface. **BFD**: • **BFD**: Enable or disable BFD on the interface. • **BFD Template**: Name of the BFD template applied to the interface. • **BFD Interval Status**: Enable or disable the BFD interval configuration.

Profile type	Description
L2 port channel profile	• **Port Configuration Profile Name**: Enter a name for the profile. • **Port Configuration Profile Description**: Enter a description for the profile. • **Channel Group Number**: Enter a number for the channel group. • **Channel Protocol**: Choose the protocol for the channel. • **Channel Group Mode**: Choose the mode for channel group. • **Description**: Description of the interface. • **Admin Status**: Enable or disable the interface. • **Layer 3**: Enable or disable switchport mode on the interface. • **Port Mode**: Select the port mode from the drop-down list.

Profile type	Description
L3 port channel profile	• **Port Configuration Profile Name**: Enter a name for the profile. • **Port Configuration Profile Description**: Enter a description for the profile. • **Channel Group Number**: Enter a number for the channel group. • **Channel Protocol**: Choose the protocol for the channel. • **Channel Group Mode**: Choose the mode for channel group. • **Description**: Description of the interface. • **Admin Status**: Enable or disable the interface. • **Layer 3**: Enable or disable switchport mode on the interface. **IPv4**: • **IP Address Type**: Choose the IP address type for the interface. **BFD**: • **BFD**: Enable or disable BFD on the interface. • **BFD Template**: Name of the BFD template applied to the interface. • **BFD Interval Status**: Enable or disable the BFD interval configuration.

Step 6 Click **Save**.

Create configuration profiles for wireless controllers

Use this procedure to create configuration profiles for wireless controllers.

Before you begin

Configuration profiles are version-specific. Configuration profiles created for a specific Cisco IOS XE Release can be applied only to wireless controllers running the same version.

Note The configuration profile workflow does not support these configurations.

- Ethernet, Wireless, and Port Channel interfaces,
- CTS Link Configuration (TrustSec),
- User Administration,
- Client Exclusion Policies (Wireless Protection Policies).

You can configure these settings in the per-device configurations. For more information, refer to Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 672.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click **Configuration profiles** > **Wireless**.

Step 3 Select the profile type, and then click **Create new**.

Step 4 Configure the required fields in the configuration profile window.

- Enter a name in the **Configuration profile name** field.
- Enter a **Description** for the profile.
- Select the **IOS XE version** for the profile.

Step 5 Click **Create**.

Step 6 Configure additional profile attributes as required for the profile type. For more information, refer to Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 672.

What to do next

You can assign the configuration profiles to wireless controllers. Refer to Manage configuration profiles, on page 1092.

Learn configuration profiles from a wireless controller

Configuration profiles standardize configuration. They also allow provisioning across multiple wireless controllers.

Catalyst Center saves the device configurations learned from a wireless controller as configuration profiles. You can assign configuration profiles to wireless controllers across networks. Configuration profiles can be learned from wireless controllers that are provisioned using either Per-Device Configurations, provisioned using intent-based network configurations, or available in the inventory without being provisioned.

Use this procedure to learn device configurations from a wireless controller and save them as configuration profiles.

Note The configuration profile workflow does not support these configurations.

- Ethernet, Wireless, and Port Channel interfaces,
- CTS Link Configuration (TrustSec),
- User Administration,
- Client Exclusion Policies (Wireless Protection Policies).

You can configure these settings in the per-device configurations. For more information, refer to Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 672.

Before you begin

- Ensure that the Cisco Catalyst 9800 Series Wireless Controller is running Cisco IOS XE Release 17.12 or later.
- Configuration profiles are version-specific. Configuration profiles learned from a wireless controller running a specific Cisco IOS XE Release can be applied only to wireless controllers running the same version.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click **Configuration profiles** > **Wireless**.

Step 3 Click **Learn from a WLC** to learn the configuration profiles from a wireless controller.

Step 4 In the **Select device** window, select the wireless controller to learn configurations from.

To view the details of the unsupported wireless controllers for learning device configurations, click **Can't find a device you're looking for?**.

Step 5 In the **Select configurations to learn** window, view the identified configurations. Update the configuration profile names, if necessary.

Step 6 In the **Review** window, review the configurations that will be saved to the configuration profiles.

Note You cannot edit the configurations in this window.

Step 7 Click **Create configuration profile** to save the configurations.

Step 8 In the **Check the results** window, verify the created profiles.

Click **View configuration profiles** to view the configuration profiles.

Manage switching device groups

Use this procedure to view and manage a switching device group.

Before you begin

Ensure that you have created a network with device groups. For more information, see Create a network, on page 1091.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click a network name in the **Networks** window.

Step 3 Expand the **Switching device groups** area.

Step 4 Use these options to manage the device groups.

If you want to...	Then...
create a device group	click **Create switching device group**. **a.** In the create window, enter a device group name. **b.** Select the devices. **c.** Click **Create switching device group**.
edit or delete a device group	click the ellipsis icon and choose **Edit device group name**, or **Delete** as needed.
view device group details	click the device group name and continue to the next step.

Step 5 Click a device group name.

The window displays the **Configurations** and **Devices** associated with the device group. Click **Provision device group** if the device group is out of sync or not yet provisioned. Refer to Provision a switching device group, on page 1103.

The **Configurations** tab displays the configuration profiles associated with the device group.

Manage the configuration profiles using the options described in the table.

Table 57: Configurations

Option	Description
Create configuration profiles	Use this option to create configuration profiles. Refer to Create a configuration profile for switching device group, on page 1093.

Option	Description
Assign configuration profiles	Use this option if there are no existing profiles assigned to the device group. **a.** Select the profile name from the drop-down list for the required profile type—Layer 2, Layer 3, Security, Network Settings, Services, and Industrial. **b.** Select the port profiles. **1.** Select the device model or individual device. **2.** Select one or more ports on the selected devices. **3.** Assign the port profile. **c.** Provision the configuration profile. Refer to Provision a switching device group, on page 1103.
Edit configuration profile assignment	In the **Configuration profile** area, use the Edit option to modify and provision the profiles. You can also use the Delete option to remove the associated profile from the device group. In the Edit window, select the required profiles or delete the existing assignment. After the required edits, provision the changes. Refer to Provision a switching device group, on page 1103.
Edit port profile assignment	In the **Port Profiles** area, click **Edit port profile assignment** to edit and provision the port profiles. You can also use the **Delete assignment** option to remove the associated profile from the device group. In the Edit window, select the required profiles or delete the existing assignment. After the required edits, provision the changes. Refer to Provision a switching device group, on page 1103.

The **Device** tab displays the list of network devices assigned to the device group. The device table includes information, such as the device name, IP address, manageability status, uptime, and so on. Click a device to view the configuration details.

If there are no devices, the **Assign devices** option is displayed.

Use these options to manage the devices.

Table 58: Devices

Option	Description
Compare configuration	Compare device configurations with an existing configuration profile. • Choose **Compare configuration** > **Compare configurations of all devices** to compare configurations of all devices. • Choose the devices you want to compare and click **Compare configuration** to compare configurations for selected devices. Refer to Compare device configurations, on page 1111.
Assign devices	Assign devices to the device group. In the Assign devices window, check the check box next to the devices you want to add and click **Assign devices**. **Note** You can assign devices only from the site associated with the network.
Remove devices	Remove the device from the device group. Check the check box next to the device you want to remove and click **Remove devices**.
Learn profiles	Create a configuration profile by learning the device configuration. Check the check box next to the device that you want to learn from and click **Learn profiles**. **Note** The learn configuration option is available for Cisco Catalyst 9000 Series Switches only. Refer to Learn configuration profiles from a switch, on page 1101.

Learn configuration profiles from a switch

Use this procedure to create a switching configuration profile by learning the configurations from a device.

Before you begin

Ensure that you have created networks and device groups and assigned devices to your device group. See Manage networks, on page 1090 and Manage switching device groups, on page 1099.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Follow these steps to learn profiles from devices.

Option 1:

a) Click a network.
b) Use one of these options to view the devices in your network.

- Under the **Device Group** tab, click a device group.

  In the **Device Group** window, click the **Devices** tab.

- Click the **Devices** tab.

c) Select the device that you want and click **Learn profiles**.

Note The **Learn profiles** option is supported only for Cisco Catalyst 9000 Series Switches.

Option 2:

a) Click **Configuration profiles** > **Switching**.
b) Click **Learn from a switch**.
c) Select the device that want to learn.

Step 3 Choose the type of configurations.

- For **Device configurations**, select the configurations to learn. Each configuration can be saved as a profile.
  - **Layer 2**
  - **Layer 3**
  - **Security**
  - **Network Settings**
  - **Services**
  - **Industrial**
- For **Port configurations**, select the ports to learn.
- For **Port channel configurations**, select the port channel to learn from.

Step 4 Click **Next**.

The configurations that are learned from the device are displayed.

Step 5 View the configurations and edit as required.

Step 6 Click **Create Configuration Profiles**.

Provision a switching device group

Assign configuration profiles to switching device groups across networks to standardize configuration and support scalable provisioning.

Before you begin

Create configuration profiles for switches and add devices to your device group. For more information, refer to Manage switching device groups, on page 1099 and Manage configuration profiles, on page 1092.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 In the **Networks** overview area, click a network name.

Step 3 In the **Switching device groups** area, click a device group name.

Choose the option that meets your requirements.

Option	Description
Provision device group	This option appears if the device group is out of sync due to configuration profile changes or assignment of new devices or profiles.
Edit configuration profile assignment	Use this option to change the configuration profile assignment for the device group or remove the existing assignment.
Edit port profile assignment	Use this option to modify the port profile assigned to the device group. You can assign a different profile or delete the existing assignment.

Step 4 In the configuration profile window, review the configuration profiles that need to be provisioned.

Assign a configuration profile or edit the existing assignment.

Table 59: Device configuration profile

If you want to...	Then...
assign a configuration profile	choose the required configuration profile from the corresponding drop-down list.
delete a configuration profile	**a.** Click the corresponding **Delete assignment** option. **b.** In the dialog box, click **Yes**.

If you want to...	Then...
select a different configuration profile	**a.** Delete the assigned configuration profile. **b.** Choose the required configuration profile from the corresponding drop-down list.

For port profiles, use these options.

Table 60: Port configuration profile

If you want to...	Then...
assign a configuration profile	**a.** Choose the port type. **b.** Select the devices. You can filter by device model or individual device. **c.** Select one or more ports on the selected devices. **d.** Choose the type of configuration profile from the **Assign port configuration profile** drop-down list. **e.** Choose the configuration profile.
unassign a configuration profile assignment	**a.** Choose the port type. **b.** Select the devices. You can filter by device model or individual device. **c.** Select one or more ports on the selected devices. **d.** Click **Unassign port configuration profile**.

Step 5 (Optional) In the **Configure device overrides** window, follow these steps to override the configuration profile attributes with device-specific values.

a) Click **Download CSV zip file**.
b) Open the downloaded CSV files and make the required edits.
c) Click **Bulk upload**, then select the modified CSV ZIP file
d) Verify the uploaded file and click **Next**.

Note When a switching feature includes child-level list entries, Catalyst Center exports or imports the child-level entries in separate CSV files.

Step 6 (Optional) In the **Review device overrides** window, check the per-device overrides for configuration profile attributes.

This window appears only if per-device configuration values differ from profile values. You can choose whether to apply the profile values or the per-device values.

Step 7 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 8 On the **Tasks** window, monitor the task deployment.

Manage devices

Before you begin

Create a network and assign devices to your network. For more information, refer to Create a network, on page 1091.

Use this procedure to view and manage devices in a campus network.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click a network name to view network details.

Step 3 Click the **Devices** tab.

Step 4 Select the required device type.

- Click **switches** to manage switches.
- Click **wireless controllers** to manage wireless controllers.

Step 5 If no devices are assigned to the network, click **Assign devices**.

For information about assigning switches, refer to Manage switching device groups, on page 1099. For information about assigning wireless controllers, refer to Assign wireless controllers to an existing network, on page 1106.

Step 6 (Optional) Click **Export** to download a comma-separated value (CSV) file containing details of the network and its devices.

Step 7 (Optional) Manage switches using these configurations:

If you want to...	Then...
learn configuration profiles from a device	Check the check box for the device to learn configurations from and click **Learn profiles**. **Note** This option is available for only Cisco Catalyst 9000 Series Switches.

If you want to...	Then...
remove devices from the network	**a.** Check the check box for the devices that you want to remove from the network **b.** Click **Remove from network**. **c.** In the dialog box, click **Remove device**.
assign devices to the network	Refer to Manage switching device groups, on page 1099.
compare device configurations	Refer to Manage switching device groups, on page 1099.

Step 8 (Optional) Manage wireless controllers using these configurations:

If you want to...	Then...
add a wireless controller to the network	click **Add WLC**. Refer to Assign wireless controllers to an existing network, on page 1106.
manage configuration profile assignments for the wireless controller	click the ellipsis icon and choose **Provision device**. Alternatively, check the check box for the device and click **provision device**. Refer to Assign configuration profiles to a wireless controller, on page 1107, Edit configuration profile assignment for a wireless controller, on page 1108, and Delete configuration profile from a wireless controller, on page 1109.
compare device configurations	click the ellipsis icon and choose **Compare configuration**. Alternatively, check the check box for the device and click **Compare configuration**. Refer to Compare device configurations, on page 1111.
view the previous comparison results	click the ellipsis icon and choose **view last run comparison**.
remove devices from the network	**a.** Click the ellipsis icon and choose **Remove from network**. Alternatively, check the check box for the device and click **Remove from network**. **b.** In the dialog box, click **Remove device**.

Assign wireless controllers to an existing network

Use this procedure to add wireless controllers to an existing network.

Before you begin

Ensure that the wireless controller is assigned to the corresponding site for the campus network.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click a network name to view network details.

Step 3 Click the **Devices** tab.

Step 4 Click **wireless controllers**.

Step 5 Complete one of these configurations:

- If there are no wireless controllers assigned to the network, click **Assign devices** to assign wireless controllers.
- If a wireless controller is already assigned to the network, click **Add WLC**.

Step 6 In the **Add device** window, select the required wireless controllers.

Step 7 Click **Assign devices**.

Assign configuration profiles to a wireless controller

If configuration profiles are not assigned to a wireless controller, use this procedure to assign configuration profiles to the wireless controller.

Before you begin

Ensure that configuration profiles are available for wireless controllers. For more information, refer to Learn configuration profiles from a wireless controller, on page 1097 or Create configuration profiles for wireless controllers, on page 1096.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click a network name to view network details.

Step 3 Click the **Devices** tab.

Step 4 Click **wireless controllers**.

Step 5 Click the device name.

Step 6 Click **Assign configuration profile** and complete these configurations in the **Assign Configuration Profiles and Provision** window:

a) In the **Assign configuration profiles** window, choose a configuration profile for each required configuration profile type from the corresponding drop-down list.

Note You can only assign configuration profiles learned from a wireless controller running the same Cisco IOS XE Release.

b) (Optional) In the **Configure device overrides** window, you can override the configuration profile attributes with device-specific values. For more information, refer to Configure per-device overrides for wireless controller configuration profiles, on page 1110.

c) (Optional) In the **Review device overrides** window, review the per-device overrides for the configuration profile attributes, if any.

This window is displayed only if there are per-device configuration values that deviate from the profile values for intersecting feature instances. You can choose the required configuration values here, either the profile values or the per-device values.

d) In the **Review** window, review the device configurations.

Catalyst Center displays any errors or warnings that may affect the provisioning workflow. You must acknowledge these issues before proceeding.

Click an error or warning link in the information banner to view its details. Use search and filters to narrow the results, or select **Export** to download the issues as a CSV file. In the details window, select the acknowledgment check box.

e) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

f) On the **Tasks** window, monitor the task deployment.

Edit configuration profile assignment for a wireless controller

If configuration profiles are already assigned to a wireless controller, use this procedure to edit the configuration profile assignment and provision the wireless controller.

Before you begin

Ensure that the required configuration profiles are available for assignment. For more information, refer to Learn configuration profiles from a wireless controller, on page 1097 or Create configuration profiles for wireless controllers, on page 1096.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click a network name to view network details.

Step 3 Click the **Devices** tab.

Step 4 Click **wireless controllers**.

Step 5 Click the device name.

Step 6 Click **Edit configuration profile assignment** and complete these configurations in the **Assign Configuration Profiles and Provision** window:

a) In the **Edit configuration profiles** window, choose a configuration profile for each required configuration profile type.

You can only assign configuration profiles learned from a wireless controller running the same Cisco IOS XE Release.

If you want to...	Then...
assign a configuration profile for a configuration profile type that doesn't have an assigned profile	choose the required configuration profile from the corresponding drop-down list.
delete a configuration profile from a configuration profile type	1. Click the corresponding **Delete assignment** option. 2. In the dialog box, click **Yes**.
choose a different configuration profile for a configuration profile type that already has an assigned profile	1. Delete the assigned configuration profile. 2. Choose the required configuration profile from the corresponding drop-down list.

b) In the **Review** window, review the device configurations.

If there is an issue that impacts provisioning, Catalyst Center displays the icon. Click the features with this icon to view error details. Edit the corresponding configuration profiles to resolve the issues before proceeding. For more information, refer to Manage configuration profiles, on page 1092.

c) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

d) On the **Tasks** window, monitor the task deployment.

Delete configuration profile from a wireless controller

Use this procedure to delete a configuration profile assignment from a wireless controller.

After deletion, you can assign a different configuration profile to the wireless controller.

Note When you delete a configuration profile from a wireless controller, Catalyst Center does not remove the corresponding configurations provisioned on the wireless controller.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
Step 2 Click a network name to view network details.
Step 3 Click the **Devices** tab.
Step 4 Click **wireless controllers**.
Step 5 Click the device name.
Step 6 Click the **Delete assignment** option to remove the configuration profile assignment for a configuration profile type.
Step 7 In the dialog box, click **Delete**.

Configure per-device overrides for wireless controller configuration profiles

Use this procedure when you want to provision a wireless controller with device-specific values overriding the configuration profile attributes.

Before you begin

Ensure that configuration profiles are available for wireless controllers. For more information, refer to Learn configuration profiles from a wireless controller, on page 1097 or Create configuration profiles for wireless controllers, on page 1096.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**
Step 2 Click a network name to view network details.
Step 3 Click the **Devices** tab.
Step 4 Click **wireless controllers**.
Step 5 Select an option to provision the device.

The **Provision Device** option appears if the device is not in a synchronized state because of a configuration profile change, or if new configuration profiles have been assigned but not provisioned.

- Click the ellipsis icon and choose **Provision Device**.
- Select the check box for the device and click **Provision Device**.
- Click the device name. In the Device window, select the **Provision Device** option.

Step 6 In the Provision window, complete these configurations.

a) In the **Edit configuration profiles** window, choose the configuration profiles to associate with the device or edit the existing assignments.
b) In the **Configure device overrides** window, follow these steps to override the configuration profile attributes with device-specific values.

1. Click **Download CSV zip file**.

   Select the profile instances you want to download. By default, all the instances are selected.

2. Open the downloaded CSV file and make the necessary edits.
3. Click **Bulk upload** and choose the modified CSV zip file.
4. Verify the uploaded file and click **Next**.

or,

1. In the left pane, choose the profile.
2. Configure the required profile attributes.
3. Click **Next**.

c) In the **Review** window, verify the changes.

The **Change type** column displays the type of change against the profile name.

d) Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

e) On the **Tasks** window, monitor the task deployment.

Compare device configurations

Use this procedure to compare device configurations with a configuration profile to identify deviations.

Before you begin

Switches

Ensure that you have created networks and device groups and assigned devices to your device group. Refer to Manage networks, on page 1090 and Manage switching device groups, on page 1099.

Wireless controller

- Ensure that a wireless controller is assigned to the network. For information, refer to Assign wireless controllers to an existing network, on page 1106.
- Ensure that configuration profile are available. For information, refer to Learn configuration profiles from a wireless controller, on page 1097.

Procedure

Step 1 From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.

Step 2 Click a network.

Step 3 Follow these steps to compare the device configurations.

Switches

a) In the **Device Groups** tab, click a device group.

b) In the **Device Group** window, choose the required option.

To...	Do this...
Compare device configurations of all the devices	Choose **Compare configuration** > **Compare configurations of all devices**.
Compare device configuration for selected devices	Check the check box for the required devices, and click **Compare configuration**.

Wireless controllers

a) In the **Devices** tab, click **wireless controllers**.

b) Click the ellipsis icon and choose **Compare configuration**.

Alternatively, check the check box for the device and click **Compare configuration**.

Step 4 In the **Compare configuration** dialog box, complete these steps:

a) From the **Select profile type** drop-down list, choose the type of configuration profile.

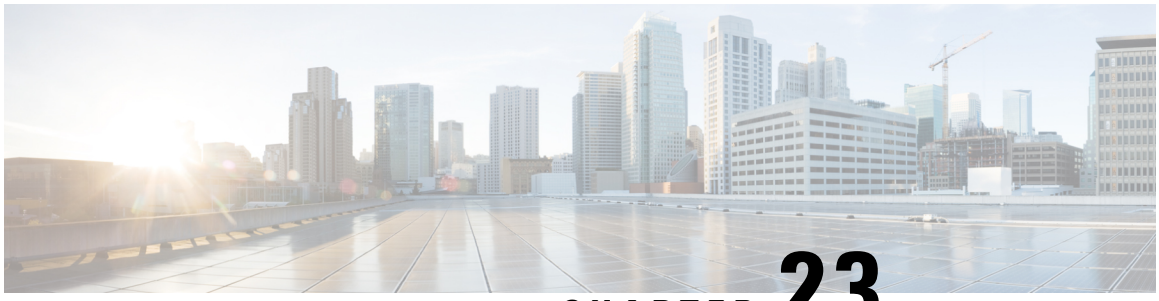
b) From the **Select profile** drop-down list, choose the profile against which you want to compare the configurations.

c) Click **Compare**.

The **Comparison results** window shows the number of devices for these comparison outcomes:

- **Match**: Devices with matching configurations.
- **Does not match**: Devices with configurations that do not match the configuration profile.
- **Comparison failed**: Devices for which the comparison failed.

You can also view the specific devices that were compared and their individual comparison results.



CHAPTER 23

Provision Services

- Applications, on page 1113
- Application hosting, on page 1134
- Application hosting on Cisco Catalyst 9100 Series Access Points, on page 1146
- Configure a site-to-site VPN, on page 1150
- Configure Cisco Umbrella, on page 1151
- Create secure tunnel, on page 1159
- Security service insertion for SD-Access, on page 1161
- Secure Equipment Access, on page 1170
- Integrate Cisco Cyber Vision Center with Catalyst Center, on page 1175

Applications

These sections provide information about applications.

About Application Visibility

The Application Visibility service lets you manage your built-in and custom applications and application sets.

The Application Visibility service, hosted as an application stack within Catalyst Center, lets you enable the Controller-Based Application Recognition (CBAR) function on a specific device to classify thousands of network and home-grown applications and network traffic.

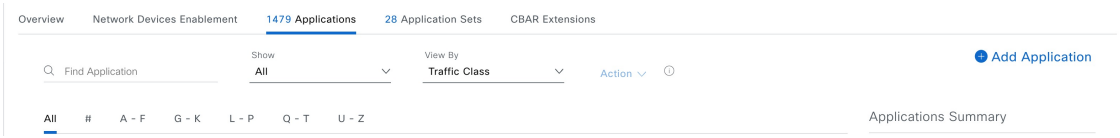
You can install these packages:

- **Application Policy**: Lets you automate QOS policies across LAN, WAN, and wireless within your campus and branch.
- **Application Registry**: Lets you view, manage, and create applications and application sets.
- **Application Visibility Service**: Provides application classification using Network-Based Application Recognition (NBAR) and CBAR techniques.

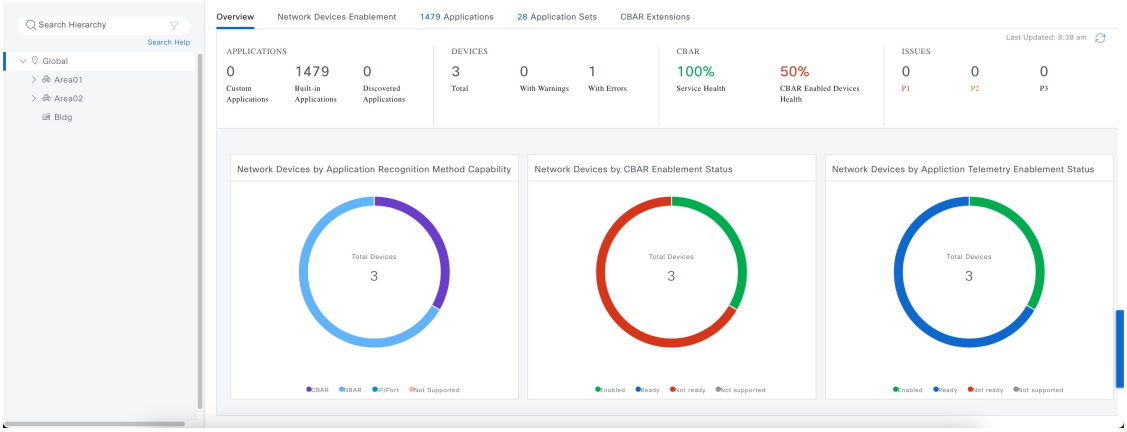
  NBAR supports provisioning of up to 450 interfaces on Cisco Catalyst 9000 devices. Catalyst Center Application Visibility does not exceed this 450-interface limit.

Note To ensure compatibility, the preceding packages must have the same package version.

If you install Application Registry or both Application Registry and Application Policy, you can see the **Applications** and **Application Sets** tabs when you click the menu icon and choose **Provision** > **Application Visibility**.



If you install Application Registry and Application Visibility Service or Application Registry, Application Policy, and Application Visibility Service, you can see the **Applications**, **Application Sets**, **Network Devices Enablement**, and **CBAR Extensions** tabs when you click the menu icon and choose **Provision** > **Application Visibility**.



Application Visibility view

This table describes the dashlets and charts that are available in the **Overview** tab in **Provision** > **Services** > **Application Visibility**.

Item	Description
Applications	This chart displays the number of applications available in the Catalyst Center application that can be used in the Application Policy. The applications are classified accordingly: • Custom: Applications added by a user • Built-in: Preinstalled applications in Catalyst Center • Discovered: Applications discovered by different recognition methods and imported into the application registry **Note** The chart shows that the applications observed only on CBAR-enabled devices.
Devices	Shows the total number of devices, devices with warning, and devices with error.
CBAR	This widget displays the service health and the average health score for all CBAR-enabled devices. The device is healthy if there are no outstanding errors or warnings on that device. The CBAR health score is calculated across all CBAR-enabled devices. You can view the CBAR health of each CBAR-enabled device. A 0% CBAR health score indicates that the device has at least one error (P1). A 50% CBAR health score indicates that the device has no errors but has at least one warning (P2). A 100% CBAR health score indicates a healthy device.
Issues	All issues are classified by priority: • Errors (P1) • Warnings (P2) • Others (P3) Click the **P1**, **P2**, and **P3** tabs to view the device issues and remedy details.
Network Devices by Application Recognition Method	This chart displays the number of devices classified by each of the application recognition methods: • CBAR: CBAR-enabled devices such as routers and switches • NBAR: NBAR-based devices such as routers, switches, Cisco Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controller • IP/port: IP/port-based devices such as switches • Not supported: Devices that aren’t supported by any of the preceding methods

Item	Description
Network Devices by CBAR Enablement Status	This chart displays the device count in each CBAR readiness status. • Enabled: Devices that are CBAR-enabled • Ready: Devices that are ready for enabling CBAR **Note** The info icon next to **Ready** status shows that the respective device is wireless enabled. • Not Ready: Devices that support CBAR but aren't ready for enabling CBAR due to some issues • Not Supported: Devices that don't support CBAR
Network Devices by Application Telemetry Enablement Status	This chart displays the device application telemetry enablement status. • Enabled: Devices that are application telemetry-enabled • Ready: Devices that are ready for enabling application telemetry • Not Ready: Devices that support application telemetry but aren't ready for enabling application telemetry due to some issues • Not Supported: Devices that don't support application telemetry

This table describes the device information and statuses that are available in **Site Devices** table, under **Network Devices Enablement** tab:

Column	Description
Device Name	Name of the device. Click the device name to view the CBAR Service Status.
Management IP	IP address of the device.
Device Type	Group of related devices, such as routers, switches and hubs, or wireless controllers.
Site	The site to which the device is assigned.
Fabric	The fabric domain to which the device is assigned.
Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Catalyst Center cannot determine a device role, it sets the device role to Unknown.
Active Recognition Method	Shows the device recognition method (CBAR, NBAR, IP/Port, or Not Supported).
OS Version	Cisco IOS software that is currently running on the device.

Column	Description
CBAR Readiness Status	If the status is Enabled, hover over the information icon to see details about whether CBAR is enabled for wireless, wired modes, or fabric SSID types. If the status is Ready, hover over the information icon to view the Remedy message.
Protocol Pack Version	Shows the current version of the protocol pack installed on the device and the protocol pack update status.
Device Registry Status	Shows the synchronization status of the device with the application registry. Hover over the info icon or the error icon to view more details about the synchronization status.
CBAR Deployment Status	Shows the CBAR deployment status. For more information, see Reconfigure CBAR on network devices, on page 1123.
Service Health Status	Click the issues in the Service Health Status column to open the CBAR Service status page, which displays a complete list of issues and the service status information of a device. If you click the Cisco Catalyst 9K device name, you can view the footprint (service load, CPU, and flows) of the CBAR service.
Application Telemetry Readiness Status	Shows the device readiness for Application Telemetry.
Application Telemetry Deployment Status	Shows Application Telemetry deployment status for the device. If the deployment fails, click the link to view the details of failure.
Application QoS Policy	The application policy applied to the device. For Cisco Wireless Controllers with more than one application policy, the number of application policies applied and the name of all the applied application policies are displayed.
WAN Interfaces	Shows the number of WAN interfaces. Click the WAN interface details to view the WAN connectivity settings for the device.
Trunk Interfaces	Shows the number of Trunk interfaces. Click the Trunk interface details to view the Trunk connectivity settings for the device.

Configure CBAR cloud

The Application Visibility service uses the CBAR cloud to enrich the protocol pack and enhance visibility for unknown applications by sending and receiving data from the cloud.

Procedure

Step 1 From the main menu, choose **Provision** > **Application Visibility**.

Step 2 Click **CBAR Extensions** tab.

Step 3 Click the **Cisco Cloud Services** link.

Step 4 The **System** > **Settings** > **External Services** > **Cisco Catalyst Cloud** page opens in a new browser tab.

a) On the **Cisco Catalyst Cloud** page, click **Register**.

b) On the **Activate your device** pop-up window, click **Next** to continue.



Note The **Activation code** field is prepopulated.

c) On the **Sign in** pop-up window, sign in to your Cisco account.

Your Catalyst Center is registered, and the **Cisco Catalyst Cloud** page displays the registration information.

Step 5 Go back to **Provision** > **Application Visibility** and select **CBAR Extensions**. Refresh the **CBAR Extensions** page.

Step 6 You can view the list of available **CBAR Dynamic Application Feeds** under **CBAR Cloud** tab. To enable all the application feeds, click **All** radio button.



Note The newly introduced application feed is automatically enabled for your network, if you select all feeds.

To enable the required application feeds:

a. Click **Selected only** radio button.

b. Check the check box next to the application feed that you want to select.

c. Click **Apply**.



Note In **Selected only** mode, the newly introduced application feeds are not imported to the network until you manually choose it.

Enable or disable CBAR cloud

Before you begin

Ensure to establish connection between Catalyst Center and Cisco Cloud Services. For more information, see Configure CBAR cloud, on page 1117.

Procedure

Step 1 From the main menu, choose **Provision** > **Application Visibility**.

Step 2 Click **CBAR Extensions** > **CBAR Cloud** tab.

Step 3 Do one of these tasks:

- To enable CBAR cloud, click the **Enable** toggle button.
- To disable CBAR cloud, click the **Enable** toggle button and click **Yes** in the subsequent dialog box.

Enable CBAR on network devices

Before you begin

- The devices must be assigned to a site.
- It is recommended to configure CBAR Cloud before enabling CBAR on the network devices. For more information, see Configure CBAR cloud, on page 1117.

Procedure

Step 1 From the main menu, choose **Provision** > **Application Visibility** > **Network Devices Enablement** tab.

The **Site Devices** table displays. To view all the columns, click the vertical ellipsis and then click **All**.

Step 2 Enable CBAR on either selected devices or all devices.

If you decide to enable CBAR on...	Then...
all devices,	**a.** From the **CBAR** drop-down list, choose **Enable CBAR on all ready devices**. **b.** In the warning dialog box, click **Yes**.
selected devices,	**a.** Check the check box next to the device name to choose the device. **b.** From the **CBAR** drop-down list, choose **Enable CBAR on selected devices**. **c.** In the warning dialog box, click **Yes**.

Step 3 After confirmation, on the **Enable CBAR** slide-in pane, review the device details and click **Enable**.

Step 4 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 5 On the **Tasks** window, monitor the task deployment.

Disable CBAR on network devices

Procedure

Step 1 From the main menu, choose **Provision** > **Application Visibility** > **Network Devices Enablement** tab.

The **Site Devices** table displays. To view all the columns, click the vertical ellipsis and then click **All**.

Step 2 Disable CBAR on either selected devices or all devices.

If you decide to disable CBAR on...	Then...
all devices,	**a.** From the **CBAR** drop-down list, choose **Disable CBAR on all devices**. **b.** In the warning dialog box, click **Yes**.
selected devices,	**a.** Check the check box next to the device name to choose the device. **b.** From the **CBAR** drop-down list, choose **Disable CBAR on selected devices**. **c.** In the warning dialog box, click **Yes**.

Step 3 After confirmation, on the **Disable CBAR** slide-in pane, schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 4 On the **Tasks** window, monitor the task deployment.

Enable Application Telemetry

Enable Application Telemetry to configure NetFlow collector settings on the devices to send traffic telemetry data for application visibility and monitoring. For more information, see About telemetry settings, on page 43.

Before you begin

We recommend that you configure CBAR Cloud before enabling Application Telemetry. For more information, see Configure CBAR cloud, on page 1117.

Procedure

Step 1 From the main menu, choose **Provision** > **Application Visibility**.

Step 2 Click the **Network Devices Enablement** tab.

Step 3 In the **Site Devices** table, do these steps to enable Application Telemetry:

a) Choose the devices.

b) From the **Application Telemetry** drop-down list, choose **Enable Application Telemetry**.

c) In the **Enable Application Telemetry** window, do these tasks:

- Click the **Generate Configure Preview** radio button and click **Preview**.
- In the **Enable Application Telemetry Task** window, Catalyst Center displays a side-by-side comparison of the running configuration and the planned configuration for the first listed device.
- Review the device configurations and then, when you're ready, click **Deploy**.
- Choose the **Now** or **Later** scheduling option and click **Deploy**.

Note The **Application Telemetry** column shows the application telemetry deployment status.

If the application telemetry deployment fails for a device, click the link under **Application Telemetry Deployment Status** column to view the failure reason.

Disable Application Telemetry

Procedure

Step 1 From the main menu, choose **Provision** > **Application Visibility**.

Step 2 Click the **Network Devices Enablement** tab.

Step 3 To disable Application Telemetry, do these steps:

a. Choose the devices in the **Site Devices** table.

b. From the **Application Telemetry** drop-down list, choose **Disable Application Telemetry** and click **Yes** in the subsequent warning dialog box.

Update the protocol pack on a CBAR-enabled device

You can upgrade the protocol pack on any device that supports CBAR to the latest or any specific protocol pack. You can update protocol pack manually or enable automatic protocol pack update.

Note

- Automatic Protocol Pack update menu is disabled when CBAR cloud connector is disabled.
- Manual Protocol Pack update menu is disabled when Automatic Protocol Pack is enabled.

Before you begin

- Configure Cisco credentials on **System Settings**. For more information about configuring Cisco credentials, see the *Cisco Catalyst Center Administration Guide*.
- Devices must support CBAR.
- CBAR must be enabled on the device.
- Protocol packs for the device must be available on cisco.com.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Network Devices Enablement** tab.

Step 3 In **Site Devices** table, check the status shown in the **Protocol Pack Version** column.

You can click the **Outdated** status to view the list of applicable protocols packs in the **Update Protocol Pack** window.

Step 4 Click **Update** corresponding to the required protocol pack version in the **Update Protocol Pack** window.

The **Protocol Pack Version** column shows **In progress** status. Click the info icon to view the current updating version. If the **Protocol Pack Version** column shows **Update failed** status, click the error icon to view the failure reason.

Step 5 If you want to manually update all the devices or selected devices to the latest protocol pack, do these tasks:

To update the protocol pack on all applicable CBAR-enabled devices:

- From the **Update Protocol Pack** drop-down list, choose **Update All Devices** and click **Yes** in the subsequent warning dialog box.

To update the protocol pack on the selected devices:

- Choose the devices in the **Site Devices** table.
- From the **Update Protocol Pack** drop-down list, choose **Update Selected Devices** and click **Yes** in the subsequent warning dialog box.

To update the protocol pack on the selected devices from the file:

- Choose the devices in the **Site Devices** table.

- From the **Update Protocol Pack** drop-down list, choose **Update Selected Devices From File**.
- In the **Update Protocol Pack From File** slide-in pane you can either drag and drop the file into the drag-and-drop area or click **Choose a file**, browse to the location of the file, and click **Open**.
- Click **Import**.

Step 6 If you want to automatically update protocol pack for all the devices, do these tasks:

- From the **Update Protocol Pack** drop-down list, enable **Auto Update** toggle button and click **Yes** in the subsequent warning dialog box.

Note By default, all ready devices are included for **Auto Update**.

To exclude selected devices from automatic protocol pack update:

- Choose the devices in the **Site Devices** table.
- From the **Update Protocol Pack** drop-down list, choose **Exclude Selected Devices** and click **Yes** in the subsequent warning dialog box.

To include selected devices for automatic protocol pack update:

- Choose the devices in the **Site Devices** table.
- From the **Update Protocol Pack** drop-down list, choose **Include Selected Devices** and click **Yes** in the subsequent warning dialog box.

Reconfigure CBAR on network devices

You can include or exclude interfaces from **Site Devices** table in the **Application Visibility** > **Network Devices Enablement** window.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Network Devices Enablement** tab.

Step 3 In the **Site Devices** table, click **Re-Configure** in the **CBAR Deployment status** column for the device that you want to configure and do these steps:

a) In the **Enable CBAR** slide-in pane, search for the device name or locate the device and click **View Interfaces**.
b) Locate the interface that you want to exclude.
c) In the **Status** column, click the toggle button to disable the interface and click **Save**.

Step 4 To include interfaces, choose **Excluded Interfaces** and enable the toggle button next to the desired interfaces, and click **Save**.

Step 5 Click **Enable**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Applications and application sets

Applications are the software programs or network signaling protocols that are used in your network. Catalyst Center supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library of approximately 1400 distinct applications.

Applications are grouped into logical groups called application sets. An application set can be assigned a business relevance within a policy.

Applications are mapped into industry standard-based traffic classes, as defined in RFC 4594, that have similar traffic treatment requirements. The traffic classes define the treatments (such as Differentiated Services Code Point [DSCP] marking, queuing, and dropping) that will be applied to the application traffic, based on the business relevance group that is assigned.

If you have additional applications that are not included in Catalyst Center, you can add them as custom applications and assign them to application sets.

Unidirectional and bidirectional application traffic

Some applications are completely symmetrical and require identical bandwidth provisioning on both ends of the connection. Traffic for such applications is described as bidirectional. For example, if 100 kbps of Low-Latency Queueing (LLQ) is assigned to voice traffic in one direction, 100 kbps of LLQ must also be provisioned for voice traffic in the opposite direction. This scenario assumes that the same Voice over IP (VoIP) coder-decoders (codecs) are being used in both directions and do not account for multicast Music-on-Hold (MoH) provisioning. However, certain applications, such as streaming video and multicast MoH, are most often unidirectional. Therefore, it might be unnecessary, and even inefficient, to provision any bandwidth guarantees for such traffic on a branch router for the branch-to-campus direction of traffic flow.

Catalyst Center lets you specify whether an application is unidirectional or bidirectional for a particular policy.

On switches and wireless controllers, NBAR2 and custom applications are unidirectional by default. However, on routers, NBAR2 applications are bidirectional by default.

Custom applications

Custom applications are applications that you add to Catalyst Center. You can view the number of custom applications available in the Overview window. For wired devices, you can define applications based on server name, IP address and port, or URL. You can define custom applications for Cisco Catalyst 9800 Series Wireless Controllers and not for Cisco AireOS controllers.

When you define an application according to its IP address and port, you can also define a DSCP value and port classification.

To simplify the configuration process, you can define an application based on another application that has similar traffic and service-level requirements. Catalyst Center copies the other application's traffic class settings to the application that you are defining.

Catalyst Center does not configure ACLs for port numbers 80, 443, 53, 5353, and 8080, even if they are defined as part of a custom application. If the custom application has a transport IP defined, Catalyst Center configures the application on the devices.

Note For a custom application to be programmed on devices when a policy is deployed, you must assign the custom application to one of the application sets defined in the policy.

Discovered applications

Discovered applications are applications that are discovered by importing from the recommended customization, such as an Infoblox DNS server, or by importing from the recommended unclassified applications flow.

The unclassified traffic can come from any flow that the CBAR-enabled device identifies, but that is not recognized by the NBAR engine. In such cases, the applications that have a meaningful bit rate are reported as unclassified and can be imported and used as applications in Catalyst Center.

The Application Visibility service lets Catalyst Center connect with external authoritative sources through the CBAR cloud to help classify the unclassified traffic or help generate improved signatures.

The available external authoritative sources are Google Meet, Service Now, Sugarcrm, Telegram, SAP, Microsoft Office 365 Cloud Connector, Box, RingCentral, Github, Crashplan, Intuit, Workday, Zscaler, Atlassian, Amazon Chime, Zoom, Dropbox, Webex, Whatsapp, Cisco Meraki, and Salesforce. This list is dynamic. As new sources are added to the cloud, the list is updated. To view the list, choose **Application Visibility** > **CBAR Extensions** > **CBAR Cloud**.

Note You must configure a CBAR cloud connector before configuring the applications.

The discovered applications are imported to the application registry.

Favorite applications

Catalyst Center lets you flag applications that you want to configure on devices before all other applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see Processing order for devices with limited resources, on page 1225.

When custom applications are created they are marked as favorite applications.

Although there is no limit to the number of applications that you can mark as favorites, designating only a small number of favorite applications (for example, fewer than 25) helps to ensure that these applications are treated correctly from a business-relevance perspective in deployments with network devices that have limited ternary content addressable memory (TCAM).

Favorite applications can belong to any business-relevance group or traffic class and are configured system-wide, not on a per-policy basis. For example, if you flag the Cisco Jabber video application as a favorite, the application is flagged as a favorite in all policies.

Keep in mind that not only can business-relevant applications be flagged as favorites, even business-irrelevant applications can be flagged as such. For example, if administrators notice a lot of unwanted Netflix traffic on the network, they might chose to flag Netflix as a favorite application (despite it being assigned as business-irrelevant). In this case, Netflix is programmed into the device policies before other business-irrelevant applications, ensuring that the business intent of controlling this application is realized.

Configure applications and application sets

These subsections describe the various tasks that you can perform in the context of applications and application sets.

Note You can edit or delete only custom and discovered applications. You can edit or delete a maximum of 100 custom and discovered applications at one instance. If you choose applications for editing or deleting, a notification message indicates the number of applications that can be edited or deleted, excluding the number of chosen applications.

Change application settings

You can change the application set or traffic class of an existing CBAR, custom, or discovered application.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click **Applications** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 Click the application name.

Step 5 In the dialog box, change one or both settings:

- **Traffic Class**: Choose a traffic class from the drop-down list. Valid traffic classes are BROADCAST_VIDEO, BULK_DATA, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, NETWORK_CONTROL, OPS_ADMIN_MGMT, REAL_TIME_INTERACTIVE, SIGNALING, TRANSACTIONAL_DATA, VOIP_TELEPHONY.
- **Application Set**: Choose an application set from the drop-down list. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 6 Click **Save**.

Create a server name-based custom application

If you have applications that are not in Catalyst Center, you can add them as custom applications.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application** at the top-right corner of the window.

Step 4 In the slide-in pane, provide the necessary information in these fields:

- **Application name**: Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.
- **Type**: Method by which users access the application. Choose **Server Name** for applications that are accessible through a server.
- **Server name**: Name of the server that hosts the application.
- **Similar to**: Application with similar traffic-handling requirements. Click the radio button to select this option, and then select an application from the drop-down list. Catalyst Center copies the other application's traffic class to the application that you are defining.
- **Traffic class**: Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- **Application set**: Application set is where you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **Save**.

Create an IP address and port-based custom application

If you have applications that are not in Catalyst Center, you can add them as custom applications.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

Step 4 In the **Application name** field, enter a name for the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.

Step 5 In the **Type** area, click the **Server IP/Port** radio button to indicate that the application is accessible through an IP address and port.

Step 6 Check the **DSCP** check box and define a DSCP value. If you do not define a value, the default value is Best Effort. Best-effort service is essentially the default behavior of the network device without any QoS.

Step 7 Check the **IP/Port Classifiers** check box to define the IP address and subnet, protocol, and port or port range for an application. Valid protocols are IP, TCP, UDP, and TCP/UDP. If you select the IP protocol, you do not define a port number or range. Click + to add more classifiers.

Step 8 Define your application traffic-handling requirements using one of these methods:

- **Similar To**: If your application has similar traffic-handling requirements as an existing application, click the **Similar To** radio-button and choose the application from the drop-down list. Catalyst Center copies the traffic class of the other application to the application that you are defining.
- **Traffic Class**: If you know the traffic class that you want to define for your application, click the **Traffic Class** radio button and choose the traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 9 From the **Application Set** drop-down list, choose the application set to which the application will belong. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 10 Click **Save**.

Create a URL-based custom application

If you have applications that are not in Catalyst Center, you can add them as custom applications.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

The **Add Application** dialog box appears.

Step 4 In the **Application name** field, enter the name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. (Underscores and hyphens are the only special characters allowed in the application name.)

Step 5 For **Type**, click the **URL** radio button.

Step 6 In the **URL** field, enter the URL used to reach the application.

Step 7 Configure the traffic class:

- To use the same traffic class as another application with similar traffic-handling requirements, click the **Similar To** radio button and choose an application from the drop-down list.
- To specify the traffic class, click the **Traffic Class** radio button and choose a traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 8 From the **Application Set** drop-down list, choose an application set in which you want the application to reside.

Step 9 Click **Save**.

Edit or delete a custom application

If required, you can change or delete a custom application.

Note You cannot delete a custom application that is directly referenced by an application policy. Application policies typically reference application sets and not individual applications. However, if a policy has special definitions for an application (such as a consumer or producer assignment or bidirectional bandwidth provisioning), the policy has a direct reference to the application. As such, you must remove the special definitions or remove the reference to the application entirely before you can delete the application.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 To edit the application:

a) Click the application name and make the required changes. For information about the fields, see Create a server name-based custom application, on page 1127, Create an IP address and port-based custom application, on page 1127, or Create a URL-based custom application, on page 1128.

b) Click **Save**.

Alternatively, choose the application and from the **Actions** drop-down list, click **Edit** to edit an application.

Note When policy is redeployed, the edited custom applications are not reconfigured on Cisco Catalyst 9800 Series Wireless Controller.

Step 5 To delete the application, click  in the application box, and then click **OK** to confirm.

Alternatively, you can do these steps to delete the application:

a) Check the check box next to an application name. You can also choose multiple applications.
b) From the **Actions** drop-down list, click **Delete** option.
c) Click **OK** to confirm.

Mark an application as favorite

You can mark an application as a favorite to designate that the application's QoS configuration must be deployed to devices before other applications' QoS configuration. An application marked as favorite has a yellow star next to it.

When you add or edit a policy, applications marked as a favorites are listed at the top of the application set.

Applications are configured system-wide, not on a per-policy basis. For more information, see Favorite applications, on page 1125.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.
Step 2 Click the **Application** tab.
Step 3 Locate the application that you want to mark as a favorite.
Step 4 Click the star icon.

Create a custom application set

If none of the application sets fits your needs, you can create a custom application set.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.
Step 2 Click the **Application Sets** tab.
Step 3 Click **Add Application Set**.
Step 4 In the slide-in pane, enter a name for the new application set.

Catalyst Center creates the new application set; however, it contains no applications.

Step 5 Choose a Default Business Relevance from the drop-down list. Default Business Relevance is the business relevance level in the absence of a concreate application QoS, this level will appear in Assurance for sites that are not assigned to a policy.

Step 6 Click **Save**.

Step 7 Use the **Search**, **Show**, or **View By** fields to locate the application set.

You can search applications based on their name, port number, and traffic class.

Step 8 Locate the applications that you want to move into the new application set.

Step 9 Check the check box next to the applications that you want to move.

Step 10 Drag and drop the applications into the new application set.

Edit or delete a custom application set

If required, you can change or delete a custom application set.



Note You cannot delete a custom application set that is referenced by an application policy. You must remove the application set from the policy before you delete the application set.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application Sets** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application set that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 Do one of these tasks:

- To edit the application set, drag and drop applications into or out of the application set. Click **OK** to confirm each change.
- To delete the application set, click  in the application set box, and then click **OK** to confirm.

Discover unclassified applications

The Application Visibility service in Catalyst Center obtains information on classified and unclassified domains and sockets from devices and displays that information in the **Observed Traffic** chart. The number of unclassified server names and IP/ports that are discovered by the Application Visibility service is shown under **Recommendations**.

You can add the unclassified server names and IP/ports to the Application Registry.

Note You can add a maximum of 1100 discovered applications in the Application Registry.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **CBAR Extensions** > **Discovered Applications** tab.

Step 3 The table lists the discovered servers or IP/ports that are not classified. Choose the server and check the **Hide Ignored Applications** check box if you want to hide the selected server or IP/ports in the table.

Step 4 Choose the server or IP/ports that you want to import as an application in the Application Registry.

Step 5 Choose the required **Application**, **Application Set**, and **Traffic Class** from the drop-down list.

Step 6 Click **Import**.

Step 7 Click the **Applications** tab and from **Show** drop-down list choose **Discovered** to view the imported application.

Application Visibility service support for the Catalyst Center Traffic Telemetry Appliance

The Catalyst Center Traffic Telemetry Appliance generates endpoint telemetry from mirrored IP network traffic and shares the telemetry data with Catalyst Center for endpoint visibility and segmentation.

The prerequisites for enabling CBAR on the Catalyst Center Traffic Telemetry Appliance include:

- The device must be assigned to a site.
- The device role must be set to **Distribution** mode.

You can configure custom applications with attribute sets and maps on the Catalyst Center Traffic Telemetry Appliance without configuring a QoS policy. For more information, see Create an application policy, on page 1231 and Deploy an application policy, on page 1237.

Discover Infoblox applications

You can integrate Catalyst Center with an organizational Infoblox DNS server to resolve unclassified traffic based on server names.

Before you begin

- The Infoblox WAPI version must be 1.5 or later. To check the Infoblox WAPI version, log in to the Infoblox server and choose **Help** > **Documentation** > **WAPI Documentation**.
- Create a role with at least Read Only permissions and assign the role to the Infoblox user. For more information, see Manage Users in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **CBAR Extensions** > **Infoblox** tab.

Step 3 Under **Infoblox**, click the **Here** link to configure IPAM/DNS server credentials in Catalyst Center.

Step 4 Complete the IPAM settings. For more information, see Configure an IP Address Manager in the *Cisco Catalyst Center Administrator Guide*.

Step 5 Go back to **Infoblox** and click the ⚙ icon to complete these settings:

- Check the **All DNS Zones** check box, or choose the required DNS zones from the **DNS Zones to Inspect** drop-down list. The drop-down list shows the DNS zones defined in the Infoblox server.
- From the **Inspect** drop-down list, choose the required inspection record.
- Check the **Read Application name from** check box and click the **Extensible Attribute** or **AVC RRTYPE format** radio button. If you click the **Extensible Attribute** radio button, enter the extensible attribute name that contains descriptive application names.
- From **Default Traffic Class**, choose the default traffic class for classifying the Infoblox applications.
- From **Default Application Set**, choose the default application set for classifying the Infoblox applications.

Step 6 Click **Save**.

Step 7 Choose the application that you want to import and complete these tasks:

- If the application does not have a name defined in the Infoblox server, edit the application name.
- Choose the required application set and traffic class from the drop-down list if you want to change the default application set and traffic class defined in the **Infoblox**.

Step 8 Click **Import**.

Step 9 Click the **Applications** tab and choose **Discovered** in the **Show** drop-down list to view or edit the imported Infoblox applications.

If you change the server name of an application after importing the application, the **Application Status** column in the **Infoblox** window shows the status of the application as **Updated**. The application name that you see in the **Application Status** column is the new server name of the application. Click the info icon to view the old server names of the application.

Edit or delete a discovered application

If required, you can edit or delete a discovered application.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Applications** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the discovered application that you want to change.

You can search for applications based on their name, port number, and traffic class.

Step 4 Do one of these tasks:

- To edit the application:
  a. Click the application name and make the required changes.

  For discovered applications, you can edit only the **Attribute Set** and **Traffic Class**.

  b. Click **Save**.

- To delete the application:
  a. Select the application and choose **Delete** option from the **Action** drop-down list at the top of the window.

  b. Click **OK** in the subsequent warning dialog box that appears on the window.

Application hosting

These sections provide information about application hosting.

About application hosting

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Catalyst Center.

You can host third-party docker applications on these platforms:

- Cisco Catalyst 9300 Series switches running Cisco IOS-XE software version 16.12.1s or later.
- Cisco Catalyst 9100 Series Access Points running Cisco IOS-XE software version 17.3.1 or later.
- Cisco Catalyst 9400 Series switches running Cisco IOS-XE software version 17.1 or later.
- Cisco Catalyst IE3200, IE3300 (4 GB), IE3400, and IE3400H Series switches running Cisco IOS-XE software version 17.3 or later.
- Cisco Catalyst IE3100 and IE 3105 Rugged Series switches running Cisco IOS-XE software version 17.15 or later.
- Cisco Catalyst IE9300 Series switches running Cisco IOS-XE software version 17.9 or later.

Note

- The disk space allocated in Catalyst Center for the hosted applications is limited to 5 GB.
- Application hosting does not support Mobility Agent (MA), N+1 redundancy, or High Availability (HA) configurations. Applications deployed through this feature are bound to the specific host device. As a result, they do not automatically migrate to redundant hardware or fail over during a device failure or maintenance event. Ensure that any critical services requiring high availability are hosted on dedicated infrastructure.

You can use these navigation paths for the wired or wireless workflow options:

- Wired/Switch Lifecycle: Navigate to **Provision** > **Services** > **Application Hosting**.
- Wireless/AP Lifecycle: Navigate to **Provision** > **Services** > **IoT Services**.

Install or update the application hosting service package

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 From the main menu, choose **System** > **Software Management**. Alternatively, click the cloud icon and click the **Go to Software Management** link.

Step 2 Under **Available Application for the release**, choose Application Hosting package and click **Install**.

Prerequisites for application hosting

To enable application hosting on a Cisco Catalyst 9000 device, these prerequisites must be fulfilled:

- Configure NETCONF port on the device before discovery.
- Configure a secure HTTP server on the device where the applications will be hosted.

  Disabling the secure HTTP server may cause the device to appear as Not Ready in Catalyst Center and result in failed application hosting operations, such as app installation.
- Configure local or AAA authentication server for HTTPS user authentication on the device. You must configure the username and password with privilege level 15.
- Ensure Cisco Catalyst 9300 Series switches are running Cisco IOS XE 16.12.x or later version and Cisco Catalyst 9400 Series switches are running Cisco IOS XE 17.1.x or later version.
- Ensure that the device has an external USB SSD pluggable storage (only for the switches of 9300 family).
- Verify that the configuration on the switch is correct. Open the WebUI on the switch and log in as the HTTPS user that is configured on Catalyst Center.

This example shows a working configuration on a switch:

```
prompt# sh run | sec ip http
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface GigabitEthernet0/0
```

Additional configuration for switches with a Cisco IOS XE release that is earlier than 17.3:

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

- On Catalyst Center, configure the HTTPS credentials while manually adding the device. The HTTPS username, password, and port number are mandatory for application hosting. The default port number is 443. You can also edit the device credentials; see Update network device credentials, on page 135. If you edit a device that is already managed, resynchronize that device in the inventory before it is used for application hosting-related actions.

Use these checks to troubleshoot credential mismatches or readiness failures:

- Validate HTTPS port settings and user privilege levels.
- Update credentials in the inventory database.
- Resync the device to re-run readiness checks.
- Interpret and address common readiness failure codes.

Note

- Application hosting HA is not supported on three-node Catalyst Center clusters.
- Application hosting does not support the Return Material Authorization (RMA) workflow.

View device readiness to host an application

You must check the readiness of the Cisco Catalyst 9300 Series switch to host the application before you can install an application on the switch.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Click **All Devices**.

Step 3 View the list of devices that are capable of hosting applications. The **App Hosting Status** indicates the readiness of the device to host an application. Click **See Details** to view the list of readiness checks performed on the device.

Application hosting readiness checks

A readiness check is a diagnostic device eligibility validation that

- verifies whether a network device is eligible for application hosting operations,
- ensures all prerequisites are met to reduce deployment failures, and
- shows the outcome statuses —Passed, Failed, or Skipped—to indicate device readiness.

Switch checks include standard application hosting criteria and a switch-specific interactive HTTPS validation.

Acess point (AP) checks require HTTP or HTTPS credentials. These checks do not display the HTTPS credential validation as a separate readiness check.

The specific readiness checks for both switches and APs include:

1. **Are HTTPS Credentials Provided in the Inventory**
2. **Does IOS-XE Version support App Hosting**
3. **Is App Hosting in Sync with the Device**
4. **Is App Hosting in Sync with the Inventory**
5. **Is Device in Managed state in the Inventory**
6. **Is Device Series Supported by Catalyst Center for App Hosting**
7. **Is HTTPS Username Configured on the Device**
8. **Is Secure HTTP Server Configured on the Device**

Table 61: Switch specific interactive HTTPS validation

Check	Action
Are HTTPS Credentials Valid	Use the **Click here** link provided in the UI to validate the HTTPS credentials configured for the device.

AP specific considerations

All AP workflows require HTTP or HTTPS prerequisites.

The interactive **Are HTTPS Credentials Valid** check does not appear as a separate readiness row for APs.

Each readiness check returns one of these statuses:

- **Passed**: The check completed successfully, and the condition is met.
- **Failed**: The condition is not met, and corrective action is required.
- **Skipped**: The check is not applicable in the current context or requires a manual validation trigger.

Operational guidelines for troubleshooting readiness check outcomes:

- If **Is App Hosting in Sync with the Device** returns a **Failed** status due to a discovery-in-progress message. Wait for the process to complete and retry.

- If **Is App Hosting in Sync with the Device** returns **Skipped** with a message indicating that the infrastructure is not enabled, proceed with the installation; the infrastructure will be enabled, and the check will re-run.
- If a check continues to fail, perform a resync from the Inventory and re-check the readiness status.

View devices and status for a selected application

Use this procedure to view all devices where a selected application is installed. You can also monitor the current application state for each device. The application-centric view in **App** > **Manage** complements the device-centric workflow in **All Devices** > **Select Device** > **View Installed Apps**.

Before you begin

You must ensure these requirements are met:

- For switches, the application hosting service must be enabled.
- For APs, the IoT Services must be enabled.
- The application must be successfully uploaded to Catalyst Center.
- The application must be installed on at least one target device.

Procedure

Step 1 From the main menu, choose one of these paths:

- Switches: Go to **Provision** > **Services** > **Application Hosting**
- Access Points: Go to **Provision** > **Services** > **IoT Services**

Step 2 Select the required application from the list.

Step 3 Click **Manage**.

Step 4 In the **Devices** view, review the application status for each device.

Step 5 Optionally, use status filters such as **ALL**, **RUNNING**, **STOPPED**, **FAILED**, or **IN-PROGRESS** to narrow your results.

Step 6 Click **Summary** to view a brief status overview of the selected application on all devices.

Step 7 Select one or more devices and use **Actions** to perform lifecycle operations.

Step 8 Click the device **Hostname** to open the device-level application view.

Information is displayed in the **Manage** view for each device:

- **Hostname**: The name of the device.
- **Device IP**: The IP address of the device.
- **Device Architecture**: The CPU architecture of the device.
- **App Version**: The version of the application currently installed.
- **App Status**: The current operational state of the application.

- **Last Heard**: The timestamp of the last communication from the device.
- **Action Status**: The status of the most recent lifecycle operation performed on the application.

Add an application

You can add a Cisco package or a docker application.

Before you begin

- **Cisco Package**: You must package the application using IOS SDK tools so that the application is compatible with IOS XE operating systems.
- **Docker**: You must save the docker image as a tar file. Enter these command to store the docker image as a tar file:

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```



Note For more information, refer to Cisco Package Format and Docker Save Command.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Click **New Application**.

Step 3 Choose the application and category from the drop-down list.

Step 4 Click **Select** and choose the application to upload.

The upload dialog validates that files are in .tar or .tar.gz format and do not exceed 2 GB before initiating the upload request.

Step 5 Click **Upload**.

You can view the newly added application in the **App Hosting** page.

Automatic download of the ThousandEyes Enterprise Agent application

The ThousandEyes Enterprise Agent application lets you monitor your network and oversee the network traffic paths across internal, external, carrier, and internet networks in real time. The advantage of the ThousandEyes Enterprise Agent application is that you do not have to import this application manually in your Catalyst Center Application Hosting Service.

When these conditions are met, the ThousandEyes Enterprise Agent application is downloaded automatically within 10 minutes of starting the Application Hosting Service:

- At least one managed device is present in the inventory, without any manageability errors.
- An inventory resync has succeeded at least once on the managed device.

To manually download the application, click this link to the ThousandEyes Enterprise Agent .tar file:

thousandeyes-enterprise-agent.cat9k.tar

If there is no internet connection, you can set a proxy connection from the console using this command:

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

Set the proxy value to connect to the ThousandEyes Enterprise Agent application.

Catalyst Center supports ThousandEyes multivariant app packages across CPU architectures. For ThousandEyes, Catalyst Center can recognize architecture-specific variants of the same app family, such as x86_64 and aarch64. It automatically resolve the right variant per device during install or upgrade and provides variant-aware lifecycle operations.

Update an application

You can update the application added in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

You can view the available applications in the **App Hosting** window.

Step 2 Choose the application that you want to update.

Step 3 Click **Update App**.

Step 4 Choose a new version of the application to be uploaded.

Step 5 Click **Upload**.

Start an application

You can start an application in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to start.

Step 4 From the **Actions** drop-down list, choose **Start App**.

Stop an application

You can stop an application in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to stop.

Step 4 From the **Actions** drop-down list, choose **Stop App**.

View applications hosted on a device

Before you begin

Complete the prerequisites in Prerequisites for Application Hosting.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

If you chose to view all devices, the **All Devices** window shows information about the devices that are capable of hosting applications, including: **Hostname**, **IP Address**, **Device Architecture**, **Image Version**, **App Hosting Status**, and **Last Updated**.

If you chose to view a list of devices for a particular application, the **Devices** window shows the information about the devices that are capable of hosting applications, including: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard, Platform Version**, and **Action Status**.

Step 3 In the **Devices** window, click **Summary** to view a summary of failed, stopped, and running applications on a device.

Step 4 To take an action on an application, click the **Action** drop-down list and choose **Start**, **Stop**, **Edit**, **Upgrade**, or **Uninstall**.

Step 5 Click the device link in which you want to view the installed hosting applications.

The **Applications** window shows the **Name**, **Version**, **App Status**, **Monitor App**, **Health**, and **Details** of the installed applications.

Note **Monitor App** contains a link to the Application Monitoring dashboard. This link is provided in the Catalyst Center application package controller .yaml file. If the file does not contain the application dashboard URL, the **Monitor App** column isn't applicable.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device.

Step 7 To download the log for a particular application, select the application and click **Application Logs**.

Step 8 To download tech support logs from the device, click **Tech Support Logs**.

Install an application using application hosting

Catalyst Center allows you to install an application on switches. For more information on the supported switches, refer to About application hosting, on page 1134.

Catalyst Center supports multi-architecture app packages across CPU architectures such as x86_64 and aarch64. It treats these as variants of the same app family. When a multi-architecture app is uploaded, Catalyst Center displays only a single app tile for all supported architectures rather than separate tiles for each architecture. On the app details page, the architecture-specific variants may appear as multiple tiles. Also, a parent app cannot be deleted while its child apps are still present.

Before you begin

- Complete the prerequisites. For more information, refer to Prerequisites for application hosting, on page 1135.
- Add the application to Catalyst Center. For more information, refer to Add an application, on page 1139.
- Check the readiness of the switch to host the application. For more information, refer to View device readiness to host an application, on page 1136.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Choose the application and click **Install**.

Step 3 In the **Get Started** window, enter a unique name for your workflow in the **Task Name** field and click **Next**.

Step 4 In the **Select Site** window, choose the site where you want to enable the application, and click **Next**.

Step 5 In the **Select Switches** window, choose the devices on which you want to install the application and click **Next**.

You can choose the devices that are in **Ready** and **Partially Ready** status. Click **See Details** to view the list of readiness checks performed on the device.

For devices that are in **Partially Ready** status, click the **Check Now** link in the **Readiness Check** window to validate the HTTPS credentials.

If you don't find your device in the **Devices Table**, click **Import** to add devices from a CSV file.

Step 6 In the **Configuration App** window, complete these settings:

- **Network Settings**:
  - From the **App-Network** drop-down list, choose a VLAN to configure the application.
  - From the **Address Type** drop-down list, choose **Static** or **Dynamic**. If you choose **Static**, click **Export** and download the CSV template. Enter the details in the CSV template. Click **Import** to upload the CSV file. If you choose **Dynamic**, enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.

- **App Resources**: Check the **Allocate all resources available on a device** or the **Customize resource allocation** check box. You can check the **Customize resource allocation** check box and modify the maximum **CPU**, **Memory**, and **Persistent Storage** values to a lower value.
- **Custom Settings**: Applicable only for Cisco package applications. Enter the configuration details for the attributes that are specified by the application.
- **App Data**: Browse and upload the application-specific files. For information about how to identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options**: Enter the docker runtime options required by the application.

Step 7 In the **Summary** window, review the application configuration settings.

Step 8 (Optional) Click **Configuration Preview** to view the configuration template used to push the configuration settings on the selected devices.

Step 9 Click **Provision**.

Step 10 In the confirmation window, click **Yes** to complete the application installation on the selected devices.

Note The installation of the application also modifies the Cisco IOS-XE configuration on the device. This change in the running configuration must be copied to the startup configuration to ensure applications function as expected after a router reload. After the application installation is complete, use the **CLI Templates** to copy the running configuration to the startup configuration.

Install applications in bulk using a CSV file

Catalyst Center enables bulk installation of applications on multiple APs.

You can import a CSV file with a list of device IPs and proceed with the application installation in a single workflow.

Before you begin

- Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9100 Series Access Points.
- Make sure that the Cisco Catalyst 9100 Series Access Points have direct IP reachability to Catalyst Center .
- Make sure that the Cisco Catalyst 9800 Series Wireless Controller is running Cisco IOS XE 17.3.x or later software.
- Make sure that the Catalyst Center appliance is running the latest Catalyst Center ISO.
- Make sure that the USB dongle is inserted in the AP.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **IoT Services**.

Step 2 Click the application you want to install on the APs.

Step 3 Click **Install**.

Step 4 In the **Get Started** window, enter the task name and click **Next**.

Step 5 In the **Input Source Selection** window, click **CSV Upload**.

Step 6 Click **Sample CSV Template** to download the file template.

Step 7 Add the list of device IPs. Alternatively, export the AP details from Inventory.

- The system supports uploading up to 500 AP IP addresses in a single CSV file for bulk application installation.
- For large AP deployments exceeding the CSV upload limit or to manage deployment risk, it is recommended to perform wave-based deployments in batches rather than a single large bulk upload.

Step 8 Use one of these options to upload the CSV file:

- Drag and drop the file to the drag and drop area.
- Click where it says **Choose a file** and select the file.

Step 9 Expand the success message to view the IP addresses validation details and click **Next**.

The duplicate IPs are shown at the bottom of the window. A preview of all the device IPs is shown at the right side of the window.

Step 10 In the **Select Access Points** window, choose the APs for hosting the application and click **Next**.

The number of invalid IPs in the uploaded CSV file is shown. You can click **View IPs** to view the invalid IPs.

Step 11 In the **Configure App** window, complete the application-specific settings and click **Next**.

Step 12 In the **Summary** window, review the app deployment configuration and click **Provision**.

If you want to modify the configuration, click **Edit** and make the required changes.

Step 13 In the **Track Provisioning Status** window, you can track the progress of the deployment. Click **View Details** to view the provisioning status and click **Next**.

Step 14 The **Done! Task Completed** window displays. Click **Manage IoT Application** to perform day-*n* tasks.

Uninstall an application from a Cisco Catalyst 9300 device

You can uninstall an application from a Cisco Catalyst 9300 Series switch.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Edit an application configuration in a Cisco Catalyst 9300 device

You can edit the application configuration if the application includes package_config.ini file and requires configuration to operate on a Cisco Catalyst 9300 Series switch.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to edit.

Step 4 From the **Actions** drop-down list, choose **Edit App Config**.

Delete an application

You can delete an application from Catalyst Center.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see Uninstall an application from a Cisco Catalyst 9300 device, on page 1144.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

You can view the available hosted applications in the **App Hosting** window.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Catalyst Center.

Otherwise, an error message shows the number of devices that are using the application. Click **Cancel** in the confirmation dialog box and uninstall the application. For more information, see Uninstall an application from a Cisco Catalyst 9300 device, on page 1144.

Download application logs

You can download application logs from Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **IoT Services**.

Step 2 Click **All Devices**.

You can view the list of devices that are capable of hosting applications.

Step 3 Click **App logs** to download the application logs from Catalyst Center.

Step 4 In the **App Logs** pop-up window, choose the application logs file that you want to download and click **Download**.

Download device tech support logs

You can download the device tech support logs from Catalyst Center for troubleshooting purposes.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **IoT Services**.

Step 2 Click **All Devices**.

A list of devices that are capable of hosting applications displays.

Step 3 Click **Tech Support logs** to download the device tech support logs.

Application hosting on Cisco Catalyst 9100 Series Access Points

These sections provide information about application hosting on Cisco Catalyst 9100 Series Access Points.

About application hosting on Cisco Catalyst 9100 Series Access Points

The move to virtual environments has prompted the need to build applications that are reusable, portable, and scalable. Application hosting gives administrators a platform for leveraging their own tools and utilities. An application, hosted on a network device, can serve a variety of purposes, such as automation, configuration management, monitoring, and integration with existing tool chains.

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Catalyst Center. This release lets you bring in the third-party SES-imagotag IoT Connector application on Cisco Catalyst 9100 Series Access Points with Cisco IOS-XE software version 17.3 or later.

The SES-imagotag IoT Connector on Cisco Catalyst 9100 Series Access Points can handle all Electronic Shelf Label (ESL) communication.

Note The access point cannot support two applications that both require the same IoT capability. If an application that uses a specific IoT feature is already running on the AP, activating another application that needs the same feature will fail because the required device is unavailable.

For example, if an application that uses the IoT radio capability of the AP is already installed and running, trying to activate another application that also needs the IoT radio capability will fail.

Application hosting workflow to install and manage USB applications on Cisco Catalyst 9100 Series Access Points

Before you begin

To enable application hosting on a device, these prerequisites must be completed:

- Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9100 Series Access Points.
- Make sure that the Cisco Catalyst 9100 Series Access Points have direct IP reachability to Catalyst Center.
- Make sure that the Cisco Catalyst 9800 Series Wireless Controller is running Cisco IOS XE 17.3.x or later software.
- Make sure that the Catalyst Center appliance is running the latest Catalyst Center ISO.
- Make sure that the USB dongle is inserted in the AP. This is required for the SES-imagotag Connector application to run.

Procedure

Step 1 Check the readiness of the Cisco Catalyst 9800 Series Wireless Controller and Cisco Catalyst 9100 Series Access Points to host the application before you install it.

For more information, see View device readiness to host an application, on page 1136.

Step 2 Install the Application Hosting service on Catalyst Center.

For more information, see Install or update the application hosting service package, on page 1135.

Step 3 Add the Cisco Catalyst 9800 Series Wireless Controller to Catalyst Center.

For more information, see Add a network device, on page 130.

Note Make sure that you enable NETCONF and set the port to 830.

You must wait for the Cisco Catalyst 9800 Series Wireless Controller to move to a Managed state.

Step 4 Assign APs to a floor on the Network Hierarchy window.

For more information, see Work with APs on a floor map, on page 256.

Step 5 Upload the USB application (the SES-imagotag Connector) to Catalyst Center.

For more information, see Add an application, on page 1139.

Step 6 Enable the IoT services.

For more information, see Enable IoT services on Cisco Catalyst 9100 Series Access Points, on page 1380.

Step 7 Configure the container as described in the Application Hosting on Catalyst APs Deployment Guide.

View installed hosting applications on Cisco Catalyst 9100 Series Access Points

Before you begin

Make sure the prerequisites have been met. For more information, see Prerequisites for Application Hosting.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **IoT Services**.

Step 2 To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

If you chose to view all devices, the **All Devices** page displays the information about the devices that are capable of hosting applications, including: **Hostname**, **IP Address**, **Image Version**, **App Hosting Status**, and **Last Updated**.

Note When the **App Hosting Status** of an AP is **Ready**, to configure the updates on the AP, check the check box next to the required hostname and click **Resync**.

If you chose to view a list of devices for a particular application, the **Devices** window shows information about the devices that are capable of hosting applications, including: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard,** **Platform Version**, and **Action Status**.

Step 3 In the **Devices** window, click **Summary** to view the summary of failed, stopped, and running applications on a device.

Step 4 Click the **Action** drop-down list to start, stop, edit, upgrade, and uninstall an application.

Step 5 Click the device link in which you want to view the installed hosting applications.

The **Applications** page shows the **Name**, **Version**, **App Status**, **IP Address**, **Health**, and **Details** of the installed applications.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device.

App details window displays the **REOURCES** and **NETWORK** information of an application.

Step 7 To download the application log, select an application for which you want to download the application log and click **Application Logs**.

Step 8 To download the tech support log, select an application for which you want to download the tech support log and click **Tech Support Logs**.

Uninstall an application from a Cisco Catalyst 9100 device

You can uninstall an application from a Cisco Catalyst 9100 Series AP.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **IoT Services**.

Step 2 Choose the application and click **Manage** to view the devices that use it.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Delete an application from a Cisco Catalyst 9100 device

You can delete an application from a Cisco Catalyst 9100 Series AP.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see Uninstall an Application From a Cisco Catalyst 9100 Device.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **IoT Services**.

You can view the available hosted applications in the **IoT Services** window.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Catalyst Center.

Otherwise, an error message shows the number of devices using the application. Click **Cancel** and uninstall the application. For more information, see Uninstall an Application From a Cisco Catalyst 9100 Device.

Configure a site-to-site VPN

You can create a site-to-site VPN and edit or delete existing site-to-site VPNs.

Catalyst Center supports site-to-site VPN on these devices:

- Cisco ASR 1000
- Cisco CSR
- Cisco ISR 4000

Create a site-to-site VPN

This procedure shows how to create a site-to-site VPN.

Before you begin

- Define the sites within the network hierarchy. See Network hierarchy, on page 229.
- Configure IP address pools to be used for the VPN tunnels. The IP address pools must have a minimum of six free IP addresses. See Configure IP address pools, on page 337.

Procedure

Step 1 From the main menu, choose **Provision** > **Site to Site VPN**.

Alternatively, you can create a site-to-site VPN from the **Workflows** > **Site to Site VPN** window.

Step 2 To create a VPN, click **Add**.
The **Choose Your Sites** workflow displays.

Step 3 In the **Choose Your Sites** workflow, do these steps:

a) Enter a VPN name in the first field.
b) Select the first site, a device in that site, and a WAN interface on that device from the Site 1 drop-down lists. The WAN interface is set by default if the device is provisioned.
c) Select the second site, a device in that site, and a WAN interface on that device from the Site 2 drop-down lists. The WAN interface is set by default if the device is provisioned.

Step 4 In the **Select Networks** window, do these steps:

a) From the **Tunnel IP Pool** drop-down list, choose an IP address pool.
b) Check the boxes next to the subnets that you want to use for each site.
c) (Optional) If you want to add a custom network for a site, click the **Add Custom Networks** link at the bottom and complete the required fields.

Step 5 In the **Configure VPN** window, do these steps:

a) Enter a preshared key for encryption.
b) Set the encryption and integrity algorithms as desired. We recommend that you use the default settings. If you change any settings, you can go back to the default choices by checking the **Use Cisco recommended IKEV2 & Transform Set Values** check box.

Step 6 In the **Summary** window, review the VPN settings. To make any changes, click **Edit**.

Step 7 To proceed, click **Create VPN**.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** window, which shows the newly created VPN.

Edit a site-to-site VPN

Procedure

Step 1 From the main menu, choose **Provision** > **Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to edit.

Step 3 Click **Edit** in the menu bar above the list.

Step 4 In the **Summary** window, review the VPN settings. To make any changes, click **Edit**.

Step 5 Click **Edit VPN** to submit the changes.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** screen.

Delete a site-to-site VPN

Procedure

Step 1 From the main menu, choose **Provision** > **Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to delete.

Step 3 Click **Delete** in the menu bar above the list.

A confirmation dialog box displays.

Step 4 Click **Yes** to confirm that you want to delete the VPN.

Configure Cisco Umbrella

These sections provide information about integrating Cisco Umbrella with Catalyst Center.

About Cisco Umbrella

The DNS-layer security in Cisco Umbrella provides the fastest and easiest way to improve your network security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

Catalyst Center supports Cisco Umbrella configuration on these devices:

- Cisco Catalyst 9800 Series Wireless Controllers with Cisco IOS-XE software version 16.12 or later
- Cisco Catalyst 9100 Series APs
- Cisco Catalyst 9200 Access Switch with Cisco IOS-XE software version 17.3.1 or later
- Cisco Catalyst 9300 Access Switch with Cisco IOS-XE software version 17.3.1 or later

Role-based access control settings for Cisco Umbrella

To configure Cisco Umbrella with Catalyst Center and to provision Cisco Umbrella on network devices, you must create a user role with the necessary RBAC permission for Cisco Umbrella. For more information, see "Manage Users" in the *Catalyst Center Administrator Guide*.

Table 62: RBAC permission matrix for Cisco Umbrella

Function	Access	Permission
Configure Cisco Umbrella with Catalyst Center	Network Design > Advanced Network Settings	Write
Add Umbrella dashlet in System 360	Network Design > Advanced Network Settings	Write
Provision Cisco Umbrella on network devices	Network Provision > Provision	Write
	Network Design > Network Hierarchy	Read
	Network Provision > Inventory Management	Read
	System	Read
	Network Provision > Scheduler	Write
	Network Services > Umbrella	Write

Configure Cisco Umbrella with Catalyst Center

Before you begin

- Create a Cisco Umbrella account.
- Log in to *login.umbrella.com* and create the necessary keys, such as the API key, legacy token, management key, and secret.

- Write down the organization ID from the Cisco Umbrella login URL.
- Create the local bypass domains in Cisco Umbrella.
- If Catalyst Center has a proxy server configured as an intermediary between itself and the network devices it manages or the Cisco cloud from which it downloads software updates, you must configure access to the proxy server. For more information, see the "Configure the Proxy" section in the Catalyst Center Administrator Guide.
- Install the Cisco Umbrella package in Catalyst Center. See the "Download and Install Packages and Updates" section in the Catalyst Center Administrator Guide.
- Create a user role with necessary RBAC permission for Cisco Umbrella. See Role-based access control settings for Cisco Umbrella, on page 1152.

Note You cannot install Cisco Umbrella package on a Catalyst Center cluster configured with IPv6.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Umbrella**.

Step 2 Enter these details that you retrieved manually from Cisco Umbrella:

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**
- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

Step 3 Click **Save**.

Add the Umbrella dashlet

You can add the **Umbrella** dashlet in the **System 360** window. The **Umbrella** dashlet shows the configuration status of Cisco Umbrella with Catalyst Center.

Before you begin

You must install the Cisco Umbrella package.

Procedure

Step 1 From the main menu, choose **System** > **System 360**.

Step 2 From the **Actions** menu, choose **Edit Dashboard** and click **Add Dashlet**.

Step 3 Choose **Umbrella Dashlet** and click **Add**.

The **Umbrella** dashlet appears under **Externally Connected Systems** in the **System 360** window. The **Umbrella** dashlet shows the status as **Available** and displays the organization ID, if Cisco Umbrella is configured with Catalyst Center.

If Cisco Umbrella is not configured with Catalyst Center, you can click the **Configure** link and complete the fields in **System** > **Settings** > **External Services** > **Umbrella**. See Configure Cisco Umbrella with Catalyst Center, on page 1152.

If the keys are changed in Cisco Umbrella, you can click the **Update** link and update the keys in **System** > **Settings** > **External Services** > **Umbrella**. See Configure Cisco Umbrella with Catalyst Center, on page 1152.

View the Umbrella service statistics dashboard

From the main menu, choose **Provision** > **Services** > **Umbrella** to view the **Umbrella Service Stats** dashboard.

The dashboard displays these dashlets:

- **Total Umbrella DNS Queries**: Shows the number of blocked DNS queries and allowed DNS queries for the selected site.
- **Blocked Umbrella DNS Queries**: Shows the number of DNS queries blocked by security policy and content policy for the selected site.

By default, the dashlet shows statistics for the last 3 hours. You can view statistics for the last 24 hours or 7 days by choosing the required time from the drop-down list in the top-left corner of the **Umbrella Service Stats** window.

Prerequisites for provisioning Cisco Umbrella on network devices

Before provisioning Cisco Umbrella on network devices, ensure that:

- Cisco Umbrella is configured with Catalyst Center.
- Wireless provisioning is complete for the devices on which you want to provision Cisco Umbrella.
- The SSID configuration is nonfabric.
- The AP is provisioned, if the device is configured with a nonfabric SSID in FlexConnect mode.
- The device has direct internet access to establish connection with Cisco Umbrella.
- The Cisco Umbrella root certificate is available in the Catalyst Center trusted certificates bundle. See the "Configure Trusted Certificates" topic in the *Cisco Catalyst Center Administrator Guide*.
- If the device has a Cisco Umbrella configuration that is not set from Catalyst Center, remove the Cisco Umbrella configuration from the device and resync the device with Catalyst Center.

Provision Cisco Umbrella on network devices

Before you begin

Make sure the prerequisites have been met. For information, see Prerequisites for provisioning Cisco Umbrella on network devices, on page 1154.

Note Cisco Umbrella deployment on your organization's network can be monitored only from *login.umbrella.com*.

Procedure

Step 1 From the main menu, choose **Workflows** > **Umbrella Deployment**.

Alternatively, do these steps:

a) From the main menu, choose **Provision** > **Umbrella**
b) Choose a site from the network hierarchy for which you want to deploy Cisco Umbrella.
c) The **Select Devices** window appears. Go to Step 4 to continue the deployment workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window displays.

a) To view the device readiness status in each site:

- **Eligible Devices**: Devices that are eligible for Cisco Umbrella configuration. See Prerequisites for provisioning Cisco Umbrella on network devices, on page 1154.
- **Enabled Devices**: Devices that are already configured from Catalyst Center.

b) Choose a site to deploy and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella can be deployed on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do these steps:

a) In the **Select Devices** window, choose the wired device.
b) In the **Configure Interface** window, do these steps:

1. Choose the ports you want to configure and click **Define Umbrella Interfaces**.
2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella** and click **Save**.

Note You must choose at lease one **IN** and one **OUT** interface to proceed further.

c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level.
d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do these steps:

a) In the **Select Devices** window, choose the wireless device.
b) Choose the SSIDs and select the required Cisco Umbrella policy for each SSID.

Note
- Only nonfabric SSIDs are listed on this page.
- If you choose an SSID and don't select the Cisco Umbrella policy, the default policy is mapped with the SSID.
- If you choose multiple policies, the order of enforcement of policies is defined in the Cisco Umbrella cloud portal.

c) In the **Umbrella Policy Association (Wireless)** window, view the default policies applied to the SSIDs.

If you want to change the policies associated with the SSIDs, click the **Cisco Umbrella** link. In the Cisco Umbrella console, you can see the network identity after you have completed the deployment of Cisco Umbrella from Catalyst Center. For devices with Cisco IOS-XE software version 16.xx, the network identity is shown as global. For devices with a Cisco IOS-XE software version later than 16.xx, the network identity is shown as a custom name created based on the site and SSID name.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 The **DNS Crypt** window appears. The **Enable DNS Packet Encryption** option is selected by default.

a) In the **DNS Crypt** window, click **Next**.
b) If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box.

Step 9 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 12 To proceed, click **Apply**.

Step 13 In the **Deployment** window, click **View Status** to view the deployment status.

You can view the Cisco Umbrella deployment status of the device and the device configuration status in Cisco Umbrella. You can also view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Disable Cisco Umbrella on network devices

Procedure

Step 1 From the main menu, choose **Workflows** > **Umbrella Deployment**.

Alternately, do these steps:

a) From the main menu, choose **Provision** > **Services** > **Umbrella**.
b) Choose a site from the network hierarchy from which you want to disable Cisco Umbrella.
c) The **Select Devices** window appears. Go to Step 4 to continue the disable workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window displays.

a) To view the device readiness status in each site:

- **Ready Devices**: Devices that meet the prerequisites for Cisco Umbrella configuration. See Prerequisites for provisioning Cisco Umbrella on network devices, on page 1154.
- **Not Ready Devices**: Devices that do not meet the prerequisites.
- **Enabled Devices**: Devices that are already configured from Catalyst Center.

b) Choose the site that you want to disable, and click **Next**.



Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is disabled on all the child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 In the **Select Devices** window, click the **Enabled** tab and choose the devices.

Step 6 Click the **Disable** radio button and choose the devices.

Step 7 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 8 To proceed, click **Deploy**.

Step 9 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 10 To proceed, click **Apply**.

Step 11 In the **Deployment** window, click **View Status** to view the deployment status.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Update the Cisco Umbrella configuration on network devices

Procedure

Step 1 From the main menu, choose **Workflows** > **Umbrella Deployment**.

Alternately, do these steps:

a) From the main menu, choose **Provision** > **Services** > **Umbrella**.
b) Choose a site from the network hierarchy for which you want to update the Cisco Umbrella configuration.
c) The **Select Devices** window displays. Go to Step 4 to continue the update workflow.

Step 2 If a task overview window displays, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window displays.

a) To view the device readiness status in each site:

- **Ready Devices**: Devices that meet the prerequisites for Cisco Umbrella configuration. See Prerequisites for provisioning Cisco Umbrella on network devices, on page 1154.
- **Not Ready Devices**: Devices that do not meet the prerequisites.
- **Enabled Devices**: Devices that are already configured from Catalyst Center.

b) Choose the site that you want to update and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is updated on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do these steps:

a) In the **Select Devices** window, choose the wired device and click the **Update** radio button.
b) In the **Configure Interface** window, do these steps:

1. Choose the ports and click **Define Umbrella Interfaces**.
2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella** and click **Save**.

Note You must choose at lease one **IN** and one **OUT** interface to proceed further.

c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level and click **Next**.
d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do these steps:

a) In the **Select Devices** window, choose the wireless device and click the **Update** radio button.

b) In the **Define Umbrella Policy Map (Wireless)** window, choose the SSIDs and choose the required Cisco Umbrella policies to map, or deselect SSIDs to disable Cisco Umbrella.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 The DNS Crypt window appears. The **Enable DNS Packet Encryption** option is selected by default.

If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box.

Step 9 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 12 To proceed, click **Apply**.

Step 13 In the **Deployment** window, click **View Status** to view the deployment status.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Create secure tunnel

Catalyst Center allows the user to plan and deploy VPN tunnels, which establish secure connections between enterprise and branch location.

Note This feature is currently supported only on the Cisco Catalyst 9300X Series Switches.

Configure secure tunnel

You can use this procedure to plan and deploy secure tunnels on day *n*.

Procedure

Step 1 From the main menu, choose **Provision** > **Secure Tunnels**.

Alternatively, you can create a secure tunnel from the **Workflows** > **Create Secure Tunnel** window.

Step 2 In the **Secure Tunnel** window, click **Create Secure Tunnel**.

Step 3 If the task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 4 In the **Select Tunnel Type** window, choose the type of secure tunnel to create by clicking the **Site To Secure Access Service Edge (SIG/SASE)** tile.

This action creates a secure tunnel between the Cisco Catalyst 9300X Series switch and the Secure Internet Gateway.

Step 5 In the **Select Secure Internet Gateway** window, click the drop-down list to choose the Secure Internet Gateway.

Do one of these tasks for the chosen Secure Internet Gateway:

- **Umbrella**: Ensure that you created a tunnel in Cisco Umbrella. You will need the tunnel ID and preshared key in the subsequent steps. For more information, see Configure Cisco Umbrella with Catalyst Center, on page 1152. If the tunnel is created in the Cisco Umbrella portal, check the confirmation check box.
- **Zscaler**: Ensure that the tunnel is already created on the Zscaler portal. After you create the tunnel in Zscaler, the preshared key and the FQDN defined there are required to configure the tunnel parameters on the selected Cisco Catalyst 9300X Series switch. If the tunnel is created in the Zscaler portal, check the confirmation check box.

Step 6 In the **Choose Site and Device** window, do these steps for site and tunnel mapping:

a. Choose the **Site** from the drop-down list.

b. Choose the **Device** from the drop-down list.

c. Choose the **Number of Tunnels** to create from the drop-down list.

d. For Zscaler, choose the **Tunnel Type** from the drop-down list.

e. Enter the **Tunnel Name**.

f. Choose the **Tunnel Source Interface**.

g. Check the check box if you want to use the same interface for the tunnel IP. If you do not want to use the same interface, uncheck the check box and choose the **Interface**.

h. Enter the **Data Center Location**.

Step 7 In **Define Tunnel Settings** window, do these steps:

a. For Umbrella, enter the **Pre-Shared Key (PSK)** for authentication.

b. If the Secure Internet Gateway integration is not complete, do these steps:

1. Enter the **Tunnel ID** and choose one of these options:
   a. **Fully Qualified Domain Name (FQDN)**: Use the **Tunnel ID** generated in Cisco Umbrella or the **User ID** generated in Zscaler.
   b. **IP Address**: Use the IP address to which you want to connect.

c. Check the check box to use the Cisco-recommended settings. To customize the values, uncheck the check box.

Step 8 In the **Configure Tunnel Traffic** window, choose from these options to route the traffic:

- **Send all traffic**: To send all traffic through the IPsec tunnel to Umbrella.
- **Send Selected Traffic**: Enter the subnet and ingress interface for the subnet. You can add more subnets by clicking .

Step 9 In the **Schedule Task** window, choose whether you want to create the tunnel now or schedule it for later. Also, you can choose to **Generate CLI Preview**.

Step 10 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 11 Click **Create Secure Tunnel**.

The **Done!** window displays.

Step 12 Click the **View all Tunnels** tab to view the status of the tunnel creation.

This process might take some time. Click **Refresh**. When the tunnel is up, the status changes from Provision to Up.

Security service insertion for SD-Access

Security service insertion enhances security for SD-Access fabric networks by steering the traffic through firewalls based on predefined policies. With security service insertion, the network acts as a security enabler by identifying and redirecting the appropriate traffic to firewalls, thus supporting a zero-trust security solution.

Security service insertion supports both wired and wireless deployments. It's compatible with Cisco and third-party firewalls.

To allow security service insertion, Catalyst Center

- performs network automation to redirect the traffic to the firewall,
- configures traffic steering policies to determine the steering of traffic to the firewall, and
- pushes the traffic steering policies to Cisco ISE and devices.

Note With the traffic steering policies to redirect the traffic configured, if the firewall IP is not reachable, then the traffic is dropped.

For information about monitoring and troubleshooting steering policy health, see "Monitor and Troubleshoot Steering Policy Health" in the *Cisco Catalyst Assurance User Guide*.

From the main menu, choose **Provision** > **Security Service Insertion** to view the **Security Service Insertion** window. It displays these details:

On...	the window displays...
day zero	• prechecks to enable a service insertion site, and • the **Enable a Service Insertion Site** option.
day *n*	• **Service insertion sites** tab, • **Steering contracts** tab, and • the **Enable Service Insertion** option.

Service insertion sites

A service insertion site is the fabric site in a network where virtual networks and firewalls are configured to steer the traffic. To use security service insertion, you must enable a service insertion site.

To use service insertion site configurations, you must enable Cisco TrustSec (CTS) policy and data download over HTTPS on the site. For more information, refer to Add Cisco ISE or other AAA servers, on page 319.

Day zero

Complete these steps on day zero to enable a service insertion site:

1. Prechecks to enable a service insertion site on day zero, on page 1162
2. Enable a service insertion site, on page 1164

Day *n*

From the main menu, choose **Provision** > **Security Service Insertion** > **Service insertion sites** to view and configure service insertion sites on day *n*.

The **Service insertion sites** tab displays these areas:

- **Summary**: displays the total number of
  - service insertion sites,
  - virtual networks used,
  - traffic steering policies, and
  - traffic steering contracts
- **Statistics by configuration**: displays this information:
  - Top five firewall IP addresses
  - Top five traffic steering contracts
  - Top five nodes
- **Service insertion sites**: displays a table with the details of the configured service insertion sites.

  Using the search bar, you can search for a service insertion site.

  Click the service insertion site name to view and edit the virtual networks and traffic steering policies associated with the service insertion site. For more information, refer to Edit a service insertion site, on page 1165.
- **Workflow library**: displays the available workflows for security service insertion.

  Click **Enable Service Insertion** to enable a service insertion site. For more information, see Enable a service insertion site, on page 1164.

Prechecks to enable a service insertion site on day zero

Use the procedure on day zero to ensure that the prerequisites to enable a service insertion site are met.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 Under **SD-Access and Access Control Application packages**, verify these configurations.

Verify if...	If not...
SD-Access and Access Control Application packages version 2.2 or later are installed.	click **Install ACA package** to install the required packages.
Cisco TrustSec (CTS) policy and data download over HTTPS are enabled on the fabric sites.	**a.** Click the hyperlinked number of fabric sites. **b.** In the **TrustSec HTTPS Download** column of the **Site readiness** dialog box, click **Not enabled** to enable the settings. For more information, refer to Add Cisco ISE or other AAA servers, on page 319.
virtual networks are configured on the required fabric sites ⚠ icon indicates that virtual networks aren't configured on the fabric sites.	click **Fabric sites** to configure Layer 3 virtual networks for the fabric site. For more information, refer to Create a Layer 3 virtual network, on page 1040.

To refresh the data, click **Refresh**.

Step 3 Under **ISE Integration**, verify these configurations.

Verify if...	If not...
Cisco ISE is integrated with Catalyst Center.	click **Integrate ISE** to integrate Cisco ISE with Catalyst Center.
Cisco ISE is running version 3.4 or later.	click **Update ISE** to update Cisco ISE to the required version.
Cisco ISE is synchronized.	click **Sync ISE** to synchronize Cisco ISE.

To refresh the data, click **Refresh**.

Step 4 Under **Security groups**, verify these configurations.

Verify if...	If not...
security groups are available.	click **Create security groups** to create the necessary security groups. For more information, refer to Create a security group, on page 1186.
Catalyst Center is managing the security groups partially or fully.	If Cisco ISE is fully managing the security groups, you can't use them for secure service insertion in Catalyst Center.

What to do next

Enable a service insertion site, on page 1164

Enable a service insertion site

Use this procedure to enable a service insertion site on a fabric site to deploy security service policies.

Before you begin

On day zero, see Prechecks to enable a service insertion site on day zero, on page 1162.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 Enable security service insertion.

- On day zero, click **Enable a Service Insertion Site**.
- On day *n*, click **Enable Service Insertion**.

Step 3 If a task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 4 In the **Select a fabric site** window, choose the fabric site that you want to enable as a service insertion site.

- View the virtual networks and devices associated with the selected fabric site.
- Verify that all the devices associated with the virtual networks are in ready state.

Note ⚠ icon indicates that the virtual network has devices that aren't in ready state. You can't configure steering policies for these virtual networks.

Step 5 In the **Service insertion deployment** window, complete these configurations.

a) From the **Virtual network** drop-down list, choose a virtual network.

b) In the **Firewall IP/mask** field, enter the firewall IP address and subnet mask.

Based on the virtual network and firewall IP address, Catalyst Center automatically generates the firewall name.

c) From the **Associated border nodes** drop-down list, choose the required border nodes.

d) (Optional) To associate another virtual network with the required border nodes, click the + icon and repeat 5.a, on page 1164 through 5.c, on page 1164.

Step 6 In the **Configure steering policies** window, choose the required steering policies.

If a steering policy is not available, click **Add policy** to add a steering policy. For more information, see Create a traffic steering policy on day n, on page 1267.

To add a steering policy, you must have at least one steering contract.

If you want to...	Then...
create a steering contract	click **Create steering contract**. For more information, see Create a traffic steering contract, on page 1270.
create a security group	hover your cursor over **Actions** and choose **Create security group**. For more information, see Create a security group, on page 1186.

Step 7 In the **Summary** window, review the configuration settings.

To make any changes, click **Edit**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Edit a service insertion site

Use this procedure to edit a service insertion site.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 In the **Service insertion sites** tab, click the service insertion site name.

Step 3 (Optional) In the **Virtual networks** tab, configure the Layer 3 virtual networks for the service insertion site.

If you want to...	Then...
add a virtual network	see Add a virtual network to a service insertion site, on page 1166.
edit virtual networks	see Edit virtual networks associated with a service insertion site, on page 1166.
delete virtual networks	see Delete virtual networks from a service insertion site, on page 1167.

Step 4 (Optional) In the **Steering policies** tab, configure the steering policies.

If you want to...	Then...
view traffic steering policies	see Traffic steering policies, on page 1266.

If you want to...	Then...
create a traffic steering policy	see Create a traffic steering policy on day n, on page 1267.
edit traffic steering policies	see Edit a traffic steering policy, on page 1268.
delete traffic steering policies	see Delete traffic steering policies, on page 1269.
deploy traffic steering policies	see Deploy traffic steering policies, on page 1270.

Add a virtual network to a service insertion site

Use this procedure to add a virtual network to an existing service insertion site.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 Click the service insertion site name.

Step 3 In the **Virtual networks** tab, click **Add new virtual network**.

Step 4 From the **Virtual network** drop-down list, choose a virtual network.

Step 5 In the **Firewall IP/mask** field, enter the firewall IP address and subnet mask.

Based on the virtual network and firewall IP address, Catalyst Center automatically generates the firewall name.

Step 6 From the **Associated border nodes** drop-down list, choose a border node.

Step 7 (Optional) To add another virtual network, click the + icon and repeat Step 4, on page 1166 to Step 6, on page 1166.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Edit virtual networks associated with a service insertion site

Use this procedure to edit virtual networks associated with an existing service insertion site.

Before you begin

Delete the associated traffic steering policies. For more information, see Delete traffic steering policies, on page 1269.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 In the **Service insertion sites** tab, click the service insertion site name.

Step 3 In the **Virtual networks** tab, check the check box next to the networks that you want to edit.

Step 4 Click **Edit**.

Step 5 In the **Edit virtual networks** slide-in pane, edit the required configurations.

For more information, see Add a virtual network to a service insertion site, on page 1166.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Delete virtual networks from a service insertion site

Use this procedure to delete virtual networks from an existing service insertion site.

When you delete a virtual network from a service insertion site, it isn't deleted from the fabric site.

Before you begin

1. Delete the traffic steering policies associated with the service insertion site.

   For more information, see Edit a service insertion site, on page 1165 or Delete traffic steering policies, on page 1269.

2. Deploy the updates on the device.

   For more information, see Edit a service insertion site, on page 1165 or Deploy traffic steering policies, on page 1270.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 In the **Service insertion sites** tab, click the service insertion site name.

Step 3 In the **Virtual networks** tab, check the check box next to the networks that you want to delete.

Step 4 Click **Delete**.

Step 5 In the warning dialog box, click **Remove**.

Step 6 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 7 On the **Tasks** window, monitor the task deployment.

Manage devices associated with a service insertion site

For a fabric site that is configured as a service insertion site, you can:

- Add an edge node to the fabric site (refer to Add a device to a fabric, on page 1022)
- Remove an edge node from the fabric site (refer to Remove a device from a fabric, on page 1025)

Note Ensure that at least one edge node is available in the fabric site.

- Add a border node to the fabric site (refer to Add a device as a border node, on page 1027)
- Remove a border node from the fabric site (refer to Remove a device from a fabric, on page 1025)

Note If the border node is associated with the service insertion site, it cannot be removed from the fabric site.

You can manage edge nodes and border nodes associated with the service insertion site. Use this procedure to manage devices associated with a service insertion site.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 In the **Service insertion sites** tab, click the service insertion site name.

Step 3 If an edge node is added to or removed from the fabric site, Catalyst Center automatically updates the service insertion site.

Step 4 If a border node is added to the fabric site, edit the virtual network to associate the border node with the service insertion site.

For information, refer to Edit virtual networks associated with a service insertion site, on page 1166.

Step 5 If a border node is removed from the fabric site, Catalyst Center automatically updates the service insertion site.

Delete a service insertion site

Use this procedure to delete a service insertion site.

Before you begin

1. If any traffic steering policies are associated with the service insertion site, delete these policies.

   For more information, refer to Delete traffic steering policies, on page 1269.

2. After deleting the traffic steering policies, deploy the updates to devices associated with the service insertion site.

   For more information, refer to Deploy traffic steering policies, on page 1270.

3. If any virtual networks are associated with the service insertion site, delete the virtual networks from the service insertion site.

   For more information, refer to Delete virtual networks from a service insertion site, on page 1167.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 In the **Service insertion sites** tab, click the service insertion site name.

Step 3 Click **Delete site**.

Step 4 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 5 On the **Tasks** window, monitor the task deployment.

Configure traffic steering contracts

Use this procedure to configure traffic steering contracts for security service insertion.

Procedure

Step 1 From the main menu, choose **Provision** > **Security Service Insertion**

Step 2 Click the **Steering contracts** tab.

Step 3 (Optional) Configure traffic steering contracts.

If you want to...	Then...
create a traffic steering contract	click **Create steering contract**. For more information, see Create a traffic steering contract, on page 1270.
edit a traffic steering contract	hover your cursor over **More Actions** and choose **Edit**. For more information, see Edit or duplicate a traffic steering contract, on page 1272.
duplicate a traffic steering contract	hover your cursor over **More Actions** and choose **Duplicate**. For more information, see Edit or duplicate a traffic steering contract, on page 1272.
delete a traffic steering contract	hover your cursor over **More Actions** and choose **Delete**. For more information, see Delete traffic steering contracts, on page 1273.

Secure Equipment Access

Cisco Secure Equipment Access (SEA) enables secure remote access to industrial OT assets. It embeds Zero Trust Network Access (ZTNA) into switches and routers, making secure remote access capabilities simple to deploy at scale. It is one of the components of the Cisco IoT Operations Dashboard (IoT OD). IoT OD is a cloud-based dashboard that

- empowers operations teams to uncover insights that help them streamline operations, and
- drive business continuity with one secure, comprehensive view of all their industrial assets.

The SEA API enables streamlined management of industrial assets by allowing easy integration and control of network devices and assets. Through RESTful capabilities, it facilitates functions like adding, monitoring, and deleting devices while ensuring secure access and data management within the IoT OD.

Application Hosting supports SEA installation on switches managed by Catalyst Center. For more information, see Install an application using application hosting, on page 1142.

SEA installation is supported on these switches:

- Cisco Catalyst IE3300, IE3400, and IE3400H Series switches running Cisco IOS-XE software version 17.3 or later
- Cisco Catalyst IE9300 Series switches running Cisco IOS-XE software version 17.9 or later, and
- Cisco Catalyst 9300 and Catalyst 9400 Series switches running Cisco IOS-XE software version 17.3 or later.

Refer to the topics in this section for a description of how to enable and configure SEA for use in your Catalyst Center deployment.

Set up the Cisco IoT Dashboard

Complete this procedure to set up the Cisco IoT Dashboard and enable Secure Equipment Access (SEA).

Procedure

Step 1 If you haven't already, create a Cisco Smart Account. Before you proceed, note your Smart Account credentials and Virtual Account.

Note For EDM-managed IR1101 and IR1800s, you must use Smart Account for PnP redirect. Additionally, Smart Account can help set up auto-population of purchased IR1101 and IR1800s devices from manufacturing to the IoT OD Organization.

Step 2 Email iotod-account-request@cisco.com to

- add and enable access to your organization, and
- enable SEA agent installation (via Catalyst Center).

What to do next

Log in to the Cisco IoT Dashboard, on page 1171.

Log in to the Cisco IoT Dashboard

Complete these steps to log in to the Cisco IoT Dashboard.

Before you begin

- Set up the Cisco IoT Dashboard, on page 1171.
- The dashboard supports the latest version of these web browsers:
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

  Use one of these browsers to log in.

Procedure

Step 1 Open one of these URLs in a supported browser:

- https://us.ciscoiot.com/
- https://eu.ciscoiot.com/

Step 2 Enter your email address and then click **Next**.

You may need to repeat this step in order to proceed.

Step 3 In the **Select your organization** window, click your organization name.

Step 4 In the **Connect Organization with Catalyst Center** screen, click **Connect**.

What to do next

Configure Secure Equipment Access, on page 1172.

Configure Secure Equipment Access

Complete this procedure to enable use of the SEA API.

Before you begin

Log in to the Cisco IoT Dashboard, on page 1171

Procedure

Step 1 In Catalyst Center, open the **Secure Equipment Access** window. From the main menu, you can either

- choose **Provision** > **Services** > **Secure Equipment Access**, or
- choose **Provision** > **Services** > **Service Catalog** and then click the **Secure Equipment Access** tile.

Step 2 Configure an API key for the SEA service.

If you want ...	Then ...
Catalyst Center to configure an API key for you,	**a.** In the **Service Connection Method** drop-down list, choose **Auto (recommended)**. **b.** In the **SEA Cluster** drop-down list, select the cluster you want to use and then click **Connect**. To choose a cluster that isn't already listed, select **Other** and then enter the cluster's URL.

If you want ...	Then ...
to generate an API key manually,	**a.** In the **Service Connection Method** drop-down list, choose **Manual**. **b.** In the browser window where you started the Cisco IoT Dashboard, complete the steps described in Generate an API key, on page 1174. **c.** Back in Catalyst Center's **Secure Equipment Access** window, paste the API key you copied into the **API Key Secret** field and then click **Connect**.

Step 3 Confirm that

- provisioning of the SEA service completed successfully, and
- your organization is listed in the **SEA Organization** area.

Step 4 Complete the Enable Remote Access wizard:

a) Start the wizard. In the **Select product family** area, choose the processor type for your Cisco devices and then click **Provision SEA Agents**.

b) Select the site where your devices reside, then click **Next**.

Note When a site is grayed out, it indicates that the site doesn't contain any devices you can deploy the SEA agent on.

c) Check the check box for the devices on which you want to deploy the SEA agent, then click **Next**.

Note
- If a device is grayed out, it's not ready for deployment. You'll need to wait until the device is ready and complete the wizard again. Click **Not Ready** status to check the errors.
- You can deploy the agent on a maximum of 10 devices at a time.

d) Configure these settings to bootstrap the SEA agent, then click **Next**:

- **Enable HTTP Connect Proxy**: Confirm that this option is selected.
- **Proxy URL**: Enter the URL of your proxy server.
- **VLAN ID**: Enter the ID of the VLAN the Management interface that (the agent? the devices? Catalyst Center?) should use.
- **IP Assignment**: Choose **Dynamic** or **Static**. If you choose **Static**, you must upload a CSV file with details.

e) In the wizard's **Summary** window, confirm the settings you specified and then click **Deploy App**.

The **Manage SEA Agents** window opens.

f) When deployment completes, confirm that `Running` is listed in each device's **Action Status** column.

Step 5 Confirm that a connection between Catalyst Center and the SEA agent running on the devices you chose is operational:

a) Return to the browser window where you started the Cisco IoT Operations Dashboard.
b) Click **System Management** from the main menu to open the **System Management** window.
c) Confirm that the devices you deployed the agent on are listed at the bottom of the window.
d) Confirm that `Up` is listed for each of these devices in the **SEA Agent Connection** column.

Step 6 Add operational technology (OT) assets:

a) Click the link for the appropriate device in the **System Management** window.
b) Open the **Add Asset** slide-in pane by clicking **+ Add Asset** in the **Assets** area.
c) Configure these settings, then click **Add**:

- **Asset Name**: Enter the asset's name.
- **IP Address**: Enter the asset's IP address.
- (Optional) **Description**: Enter a description of the asset.

d) Confirm that the asset you added is listed in the **Assets** area.
e) Repeat Steps 6a through 6d for each OT asset you want to add.

Step 7 Configure the access method for the OT assets you just added:

a) Click the link for an asset.
b) Open the **Add Access Method** slide-in pane, by clicking **+ Add Access Method** in the **Access Methods** area.
c) Configure these settings, then click **Add**:

- **Access Method**: Choose the access method you want to use from the drop-down list.
- **Port**: Enter the port to use.
- **Session Timeout**: Specify how much time must pass before a session times out due to inactivity.
- **Username** and **Password**: Enter the appropriate login credentials.
- **Name**: Enter a name for the access method you're configuring.
- (Optional) **Description**: Enter a description of the access method.

d) Confirm that the access method you added is listed in the **Access Methods** area.
e) Repeat Steps 8a through 8d for each access method you want to add.

Step 8 Establish a remote session with one of the access methods you just created:

a) From the Cisco IoT Operations Dashboard's main menu, click **Remote Sessions**.
b) In the tile for the access method you want to use, click **Connect**.
c) Enter the login credentials configured for the access method.

Generate an API key

Complete these steps to generate an API key.

Before you begin

Log in to the Cisco IoT Dashboard, on page 1171.

Procedure

Step 1 In the top-right corner of the Cisco IoT Dashboard, click the drop-down list that displays your login name and then click **Access Control**.

Step 2 In the **Access Control** window, click the **API Key** tab.

Step 3 Click the **Generate API Key** link.

Step 4 Enter this information and then click **Generate**:

- **Name**: Enter a name for the API key.
- **Role**: Enter the appropriate user role.
- **Expiration**: Choose how long this API key will remain valid.

Step 5 At the bottom of the **Generate API Key** window, click the copy icon to copy the API key that was just generated.

Integrate Cisco Cyber Vision Center with Catalyst Center

Catalyst Center supports integration with Cisco Cyber Vision, which is a network security solution. The browser-based manager is called Cisco Cyber Vision Center. The Cyber Vision Center helps monitor and manage network devices.

The Cisco Cyber Vision feature appears under **Provision** > **Services** menu in Catalyst Center UI after you install the **Industrial App Orchestrator** package in Catalyst Center. For more information, see Download and install applications in Cisco Catalyst Center Administrator Guide.

The Cyber Vision app with active discovery support (for example, CiscoCyberVision-IOx-Active-Discovery-aarch64-5.2.0.tar) is bundled by default on the Catalyst Center. The simplified Cyber Vision app deployment workflow supports this app. You may upload the Cyber Vision app without active discovery support (for example, CiscoCyberVision-IOx-aarch64-5.2.0.tar) to the Application Hosting in Catalyst Center. This app has a different application name, application ID, and requires a Cyber Vision deployment token; therefore, the simplified Cyber Vision app deployment workflow is not supported. To deploy this app on IE devices, use the standard app deployment workflow and manually provide all required deployment parameters.

Cyber Vision app deployment is supported on IE3300, IE3400, IE3400H, IE3500, IE3500H, and IE9300 Rugged Series switches.

Manage Cyber Vision Centers

You can add, edit, and remove Cyber Vision Centers in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Cisco Cyber Vision**.

Step 2 Read the **Instructions for obtaining the token for a Cyber Vision Center** and generate the deployment token.

For more information, see Deployment tokens in the Cisco Cyber Vision GUI Administration Guide

Add Cyber Vision Center

Step 3 From the **Manage Centers** drop-down list, choose **Add**.

Step 4 In the **Add Cyber Vision Centers** window, enter the **Name**, **Hostname/IP Address**, and **Token** for the Cyber Vision Center. Click **Add**.

You can click **Add Row** to add up to 20 Cyber Vision Centers.

Edit Cyber Vision Center

Step 5 From the **Manage Centers** drop-down list, choose **Edit**.

Step 6 Edit the **Name** and **Hostname/IP Address** as required and click **Save**.

You can edit the **Hostname/IP Address** only if there are no sensors associated with the Cyber Vision Center.

Step 7 In the **Save Changes** warning message, click **Save**.

Remove Cyber Vision Center

Step 8 From the **Manage Centers** drop-down list, choose **Remove**.

Step 9 Choose the Cyber Vision Center and click **Remove**.

You can remove the Cyber Vision Center only if there are no sensors associated with it.

Deploy sensor for Cyber Vision Center

You can deploy Cyber Vision sensor Apps on switches managed by Catalyst Center.

Before you begin

Ensure that these prerequisites are completed:

- Check the supported hardware and software versions for the switches.
- Format or partition the SD card present on the switches.
- Configure the uplink interface and route on the switches to ensure that the Cyber Vision Center is reachable
- Synchronize the date and time of the NTP server on the switches with the Cyber Vision Center
- Enable HTTPS, SSH, or both protocols on the switches.
- Capture VLAN is not included in any physical interface or trunk other than AppGigabitEthernet1/1 interface.

- Push the prerequisite configuration to the switches using the CLI template before deployment. For more information, see Initial Configuration in the Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide.
- Ensure that the Cyber Vision Center deployment token added in the Catalyst Center is currently valid and has not expired or run out of usage count.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Cisco Cyber Vision**.

Step 2 Click **Deploy Sensor Apps** corresponding to the Cyber Vision Center on which you want to deploy sensor Apps.

Step 3 Complete the prerequisites listed in the **Review Prerequisites** window and click **Next**.

Step 4 In the **Select Site** window, choose the site where you want to deploy the sensor and click **Next**.

Step 5 In the **Select Switches** window, choose the switches to deploy the Cyber Vision sensor App and click **Next**.

You can select up to 10 switches at a time.

Step 6 In the **Configure Network** window, complete the **Collection Interface** and **Capture Interface** settings. Click **Next**.

The collection interface handles sensor communication. The capture interface monitors traffic.

Step 7 In the **Summary** window, review the configuration and click **Deploy App**.

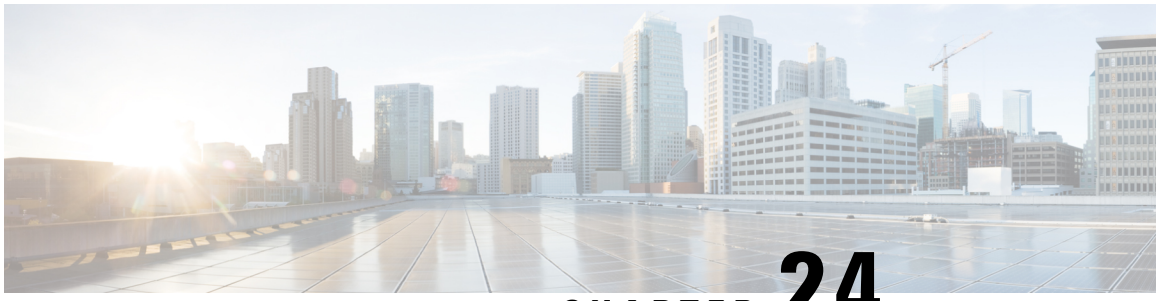
The deployment status is shown in the **Application Hosting** page. For more information, see View applications hosted on a device, on page 1141.



PART VI

Configure Policies

- Configure Group-Based Access Control Policies and Analytics, on page 1181
- Configure IP-Based and URL-Based Access Control Policies, on page 1209
- Configure Application Policies, on page 1217
- Configure Traffic-Copy Policies, on page 1247
- Configure Rule-Based Compliance Policies, on page 1253
- Configure Traffic Steering Policies, on page 1265



CHAPTER 24

Configure Group-Based Access Control Policies and Analytics

- Group-based access control, on page 1181
- Cisco Group-Based Policy Analytics, on page 1195

Group-based access control

Catalyst Center implements Software-Defined Access (SD-Access) in two ways:

- Virtual networks (VNs) provide macro-level segmentation, such as to separate IoT devices from the corporate network.
- Group-based policies provide micro-level segmentation, such as to control what types of network traffic to permit or deny between engineering and HR groups.

Group-based access control policies provide these benefits:

- Rich identity-based access control functionality with network automation and assurance benefits.
- Granular access control.
- Security groups apply to all virtual networks, which simplifies policy management.
- Policy views help you to understand the overall policy structure, and create or update required access control policies.
- Eliminates the need to switch between different applications to manage security groups and define protected assets.
- Provides enhanced features for deploying enterprise-wide access control policies.
- Restricts lateral movement of threats like ransom ware before you have identity or Network Admission Control (NAC) applications in place.
- Provides an easy migration path to Cisco Identity Services Engine (Cisco ISE) for users who are using third-party identity applications, but want to move to Cisco ISE.

For information about creating IP pools, sites, and virtual networks in Catalyst Center, see the *Catalyst Center Administrator Guide*.

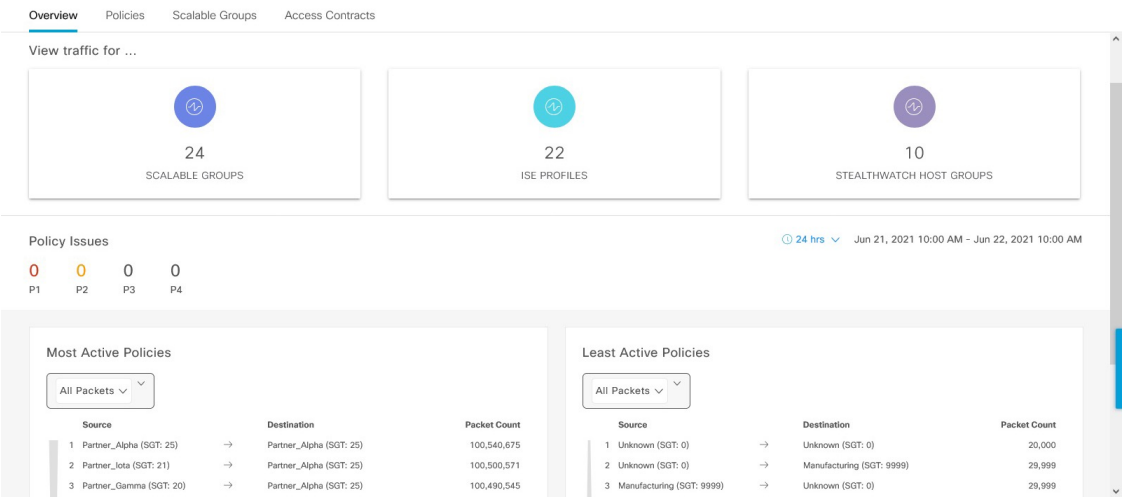
For information about configuring Catalyst Center for Cisco ISE, see the *Catalyst Center Installation Guide*.

For information about configuring Cisco ISE for Catalyst Center, see the Cisco Identity Services Engine Administrator Guide.

Group-Based Access Control Policy dashboard

The Group-Based Access Control Policy dashboard provides you with a summary of network activity, policy-related issues, and traffic trends. From the main menu, choose **Policy** > **Group-Based Access Control** > **Overview** to view this dashboard.

Figure 29: Group-Based Access Control Policy dashboard



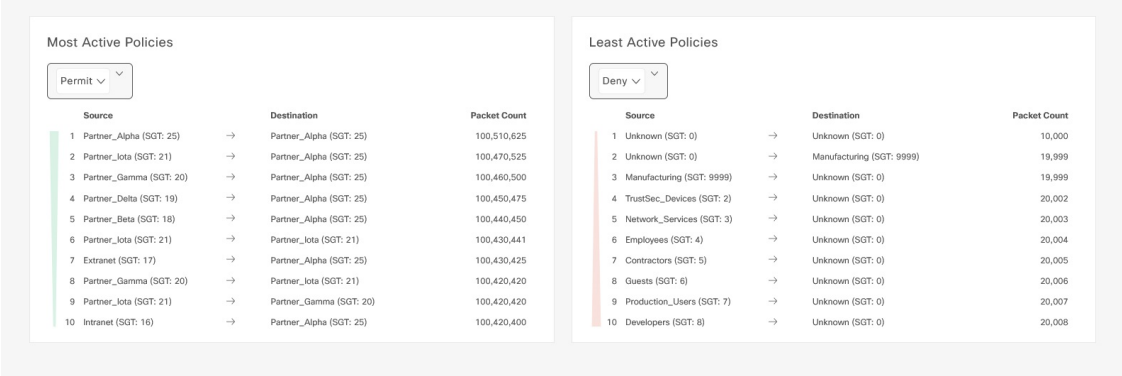
You can view these details in this dashboard:

- **View Traffic**: You can view the traffic for security groups, Cisco ISE profiles, and stealthwatch host groups. You must install the Group-Based Policy Analytics package to view this data. Group-Based Policy Analytics provides you with insights to create group-based policies by visualizing communications between assets in order to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies. Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network, and their communication. For more information, see Cisco Group-Based Policy Analytics, on page 1195.
- **View Policy-Related Issues**: It displays a count of policy-related issues. Click a counter to view the details. It opens the **Assurance Issues** dashboard in a new browser tab, where you can view the details.

Note This view of policy-related issues is for the currently selected time period. Use the time selector to adjust the time window, as needed.

- **View Most Active and Least Active Policies**: It provides the details about the most active and least active policies. By default, this view is based on the count of total number of packets seen in the network for each policy (for each source-to-destination group pairing). You can use the drop-down list to select only the permitted packets or dropped packets. You can use the dropped packets option to see which policies are enforcing policy-based drops most actively.

Figure 30: Most Active Policies and Least Active Policies dashlets



Note This view of policy activity is for the currently selected time period. Use the time selector to adjust the time window, as needed.

Group-based access control policies

Access control policies define which network traffic can pass from a source security group to a destination security group.

- **Security Group**: A classification category to which you can assign users, network devices, or resources. Security groups are used in access control policies. You can associate security groups with virtual networks based on your organization's network configuration, access requirements, and restrictions.
- **Contract**: An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination security groups. In other words, a contract is a traffic filter definition. Access contracts define the actions (permit or deny) that are performed when the traffic matches a network application, protocol, and port. The default action is to use the catch all rule when no other rules match.
- **Group-Based Access Control Policies**: A group-based access control policy identifies a specific source and destination group pair and associates an access contract. The access contract specifies what types of traffic are permitted or denied between the source group and the destination group. These policies are unidirectional.

  Security groups and access contracts are the basic building blocks of access control policy. While creating an access control policy, you can use the security groups and contracts that you have created earlier, or create new security groups and contracts while creating the policy. If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, if you want to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups. For example, if you want to specify the network resources that can be accessed by the users associated with the Contractors source security group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the Finance Servers destination security group, you can create an access control policy with single destination and multiple source groups.

You can specify the default policy to be used when no contract is specified for a source and destination security group combination. The default policy is **Permit**. You can change this policy to **Deny**, **Permit_IP_Log**, or **Deny_IP_Log**, if necessary. You can set the default policy based on your network type—an open or closed network.

Note We recommend that you change the default policy from **Permit** to **Deny** only if you have created explicit policies to permit necessary network traffic for all your network infrastructure devices. Failure to do so can result in loss of network connectivity.

List view

Click the **List** icon at the top-right corner of the **Group-Based Access Control** window to launch the **List** view.

- **Source View**: Displays a list of existing policies that are organized based on the source groups. You can expand each row to view the specific source-destination policy details.
- **Destination View**: Displays a list of existing policies that are organized based on the destination groups. You can expand each row to view the specific source-destination policy details.

To see which destination groups are available from a specific source group, use the **Source** view. To see which source groups are permitted to access a particular destination group, use the **Destination** view. For example, to see which destination groups are available to users who are part of the Contractors source security group, use the **Source** view. To see which source groups can access the Finance Servers destination security group, use the **Destination** view.

You can also view the policy enforcement statistics data in the policies listing table. The total number of permitted and denied policies display for the selected time period.

The policy enforcement statistics are collected from the network devices that are provisioned for group-based policy and telemetry data language (TDL) subscription. These configurations are normally provisioned automatically for network devices that are part of a fabric. Manual configuration can be done for nonfabric network devices.

Consider these points while using the policy enforcement statistics data:

- Policy enforcement statistics data is available only when the Group-Based Policy Analytics package is deployed.
- Telemetry subscription is added as part of base provisioning for both fabric and nonfabric network devices. The TrustSec enforcement action is invoked when a new network device is added to Catalyst Center and assigned to a site.
- Software-Defined Access (SD-Access) adds TrustSec enforcement for the network devices that are added to a fabric. TrustSec telemetry data is collected only when this enforcement is enabled on a network device. If it is not enabled, the telemetry subscriptions used for policy monitoring are used to collect the TDL data for TrustSec.
- Cisco IOS XE 16.12 and later supports TDL streaming data.
- NETCONF must be enabled on the network devices.

- This configuration must be added manually for the nonfabric network devices:

```
cts role-based enforcement vlan-list <VLAN of the endpoints>
```

- After upgrading, you will see this message in the **Provision > Network Devices > Inventory** window:

```
We detected IOS-XE devices in your network where new telemetry subscription for assurance
data needs to be enabled and some of the existing subscription needs to be optimized
for performance. Please note that you will have to enable netconf and configure the
netconf port in the Inventory credentials for these devices. Also note that these devices
will receive a new subscription for group based policy monitoring telemetry. Do you
want to take an action to provision these subscriptions?
```

  Click **Apply Fix** to push the configuration to all the network devices with site assigned.

Matrix view

Click the **Grid** icon at the top-right corner of the **Group-Based Access Control** window to launch the Matrix view. The Matrix view is a core policy view that provides an overview of all the policies for all the security groups (whether explicit or default). You can use the Matrix view to view all the source and destination policies and understand the overall policy structure. You can view, create, and update access control policies from the Matrix view.

The Matrix view contains two axes:

- Source axis: The vertical axis lists all the source security groups.
- Destination axis: The horizontal axis lists all the destination security groups.

Place the cursor over a cell to view the policy for a given source security group and a destination security group. The color of a cell is based on the policy that applies to that cell. Colors indicate which policies are applied to each cell, including:

- **Permit**: Green
- **Deny**: Red
- **Custom**: Gold
- **Default**: Gray

Place the cursor over the **Permit**, **Deny**, **Custom**, or **Default** icon that displays at the top of the matrix to view the cells to which the policy is applied.

The Matrix view highlights a cell and the corresponding row (source security group) and column (destination security group) when a cell is selected. The coordinates (source and destination security groups) of the selected cell display near the matrix content area.

Click a cell to open the **Create Policy** or **Edit Policy** slide-in pane for that cell. The **Create Policy** slide-in pane shows the source and destination security groups as read-only fields. You can only update the policy status and access contract for that cell.

You can create custom views of the policy matrix to focus only on the policies that you are interested in. To do this, from the **View** drop-down list, choose **Create View**. While creating a custom view, you can specify the subset of the security groups that you want to include in the custom view. You can save the custom views and edit them later, if required. From the **View** drop-down list, choose **Manage Views** to create, edit, duplicate, or delete custom views. The **Default View** shows all the source and destination security groups.

You can navigate through the matrix by dragging the cursor over the matrix content area, or by using the horizontal and vertical scroll bars. You can also use the mini-map to navigate through the matrix. The mini-map helps you to easily navigate through the matrix when the matrix size is large and extends beyond the screen size. You can move and place the mini-map anywhere on your screen. The mini-map provides the whole matrix view. The light gray portion in the mini-map represents the portion of the matrix that is currently displayed on your screen. You can drag your cursor over that area to scroll through the matrix.

Note The mini-map is closed by default. Click the **Expand** icon to expand and view the mini-map.

Use the **Filter** option to view a subset of the policy matrix for the selected set of source and destination groups. You can create a filter to focus only on the policies that you are interested in. To create the filter, select the source and destination groups that you want to include.

Policy creation overview

1. Define the categorizations for your organization or the portion of your organization that you plan to start with.
2. Create security groups for the categorizations that you identified.
3. Create access contracts for the types of network traffic that you wish to control. There are predefined sample access contracts to Permit or Deny all traffic, and also some example contracts showing more specific traffic filtering. You can create additional, more granular access contracts based on specific application definitions.
4. Decide which categories of network users require access to particular network resources, such as application servers and connections to other networks.
5. Create access policies, associate a source group, a destination group, and an access contract, to define how traffic is allowed to flow from the source to the destination.

Create a security group

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Security Groups**.

Step 2 Click **Create Security Group**.

Step 3 In the **Create Security Group** slide-in pane, enter a name and description (optional) for the security group.

Note These characters are supported for the **Name** field:

- alphanumeric characters
- underscore (_)

The security group name must start with an alphabetic character.

Catalyst Center generates the tag value. You can update this value, if necessary. An error message is displayed if the value that you specified is already used by an existing security group. The valid range is from 2 to 65519.

Step 4 From the **Virtual Networks** drop-down list, choose the virtual networks to be associated with this security group. By default, the default virtual network is selected.

Note When Catalyst Center 2.3.3 or later is integrated with Cisco ISE 3.2 or later, security groups are not associated with virtual networks, and the **Virtual Networks** field do not display for these releases. However, if you are using Cisco ISE 3.1 or earlier, the security group and virtual network association details display.

Step 5 Check the **Propagate to ACI** check box if you want the security group to be propagated to Cisco Application-Centric Infrastructure (ACI).

Step 6 Choose whether you want to create the security group now or schedule it for later.

If the **Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Catalyst Center, see the *Cisco Catalyst Center ITSM Integration Guide*.

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Security Groups** window. Click the task status link to view the task details in **Activities** > **Tasks**. You can edit or cancel a task before it is executed.

Note You cannot create a security group with the name ANY or the tag value 0xFFFF/65535. Security Group ANY/65535 is a reserved internal security group that is used for the Catalyst Center default policy.

Edit a security group

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Security Groups**.

Step 2 In the **Security Groups** window, check the check box next to the security group that you want to edit, and then click **Edit**.

Step 3 In the **Edit Security Group** slide-in pane, after making the necessary changes:

- Click **Save Now** to save the changes immediately.
- Click **Schedule Later** to schedule the update at a specific time. In the **Scheduler** slide-in pane, specify the start time, date, and time zone, and then click **Apply**.

When you update the security groups, you must deploy the changes on the network devices. Click **Deploy Now** to deploy the changes immediately, or click **Deploy Later** to deploy the changes later.

Delete a security group

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Security Groups**.

Step 2 Check the check box next to the security group that you want to delete.

Step 3 Choose one of these options:

- To delete the security group immediately, click **Delete Now**.
- To delete the security group later, click **Delete Later**. In the **Schedule Delete** slide-in pane, specify the start time, date, and time zone, and then click **Apply**.

Note Click the link in the **Policies** column of a security group to view the access control rules using that security group and the policy to which it belongs. You cannot delete a security group if it is used in any access policy.

Synchronization of security groups between Catalyst Center and Cisco ISE

While synchronizing the security groups in Catalyst Center with Cisco ISE:

- If a security group is present in Catalyst Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a security group is present in Cisco ISE and is not present in Catalyst Center, it is created in Catalyst Center.
- If a security group name is the same in both Catalyst Center and Cisco ISE, but the description and ACI data are different, Catalyst Center is updated with the data specified in Cisco ISE.
- If a security group name is the same in Catalyst Center and Cisco ISE, but the tag values are different, a new security group with the tag value specified in Cisco ISE is created in Catalyst Center. The name of the existing security group in Catalyst Center is updated with the suffix **_DNAC**.
- If a tag value is the same but the security group name is different, the security group name in Catalyst Center is updated with the name specified in Cisco ISE.

An orange triangle icon displays next to a security group if synchronization with Cisco ISE is not completed.

Cisco ISE supports the packets coming from ACI to the TrustSec domain by synchronizing the Internal Endpoint Groups (IEPGs) and creating correlating read-only security groups in Cisco ISE. These security groups are displayed in the **Security Groups** window with the value **ACI** in the **Created In** column. You cannot edit or delete the security groups that are learned from ACI, but you can use them in the policies.

The **Associated Contracts** column shows the associated contracts for the security groups that are learned from ACI. Click the link displayed in the **Associated Contracts** column to view the details about the associated contracts.

When an IEPG is updated in ACI, the corresponding security group configuration is updated in Cisco ISE. A new EEPG is created in ACI when a security group is created in Cisco ISE.

Create an access contract

An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination security groups. Access contracts define the actions (permit or deny) that are performed when the traffic matches a network application, protocol, and port.

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 Click **Create Access Contract**.

Step 3 In the **Create Access Contract** slide-in pane, enter the required details.

The **Modeled Access Contract** check box is enabled by default. This enables Catalyst Center to generate the valid commands for the underlying Security Group ACLs (SGACLs). When this option is enabled, the access contract is based on a model that allows you to create and edit without the need to know the underlying command line syntax.

Uncheck the **Modeled Access Contract** check box if you want to enter the SGACL command lines directly and store the access contract as text. Syntax checking is not done for the command line text that you enter. You must ensure that the command syntax is valid.

Note

- You can enable or disable this option only at the time of creating the access contracts. You cannot update this option for the existing access contracts.
- Some of the advanced SGACL commands might not be supported on all Cisco network devices.

Step 4 Create the traffic filter rules:

- From the **Action** drop-down list, choose **Deny** or **Permit**.
- From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

  If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option from the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the **+** symbol and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the handle icon at the left end of a rule to drag and change the order of the rule.

You can enable or disable logging for any traffic filter rule (including the default action) by using the **Logging** toggle. Logging is disabled by default. When logging is enabled, the network device sends a syslog message when the traffic filter rule is hit. This might be helpful in troubleshooting and initial testing of a policy. However, we recommend that you use this option sparingly because it might have a resource and performance impact on the network devices.

Step 5 From the **Default Action** drop-down list, choose **Deny** or **Permit**.

You can enable logging for the default action, if required.

Step 6 Choose whether you want to create the access contract now or schedule it for later.

If the **Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Catalyst Center, see the Cisco Catalyst Center ITSM Integration Guide.

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Access Contract** window. Click the task status link to view the task details in **Activities > Tasks**. You can edit or cancel a task before it is executed.

Edit an access contract

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 In the **Access Contracts** window, check the check box next to the access contract that you want to edit.

Step 3 Choose **Actions > Edit**.

Step 4 In the **Edit Access Contract** window, after making the necessary changes, choose whether you want to update the access contract now or schedule it for later.

You can use the **Filter** option to search for the contracts.

You can duplicate an existing access contract and create a new access contract by editing the required details. When you duplicate an access contract, all information in the existing access contract is copied and the copied contract has the existing contract name with the string **Copy** appended at the end. Click **Save Now** to create the duplicate contract immediately, or click **Schedule Later** to create the duplicate contract later.

When you update the security groups, contracts, or policies, you must deploy the changes on the network devices. If you update the policies and do not deploy the updated policies, notifications about the policy changes are not sent to the network devices, and the policies that are currently active in the network may not be consistent with the policy information displayed in Catalyst Center. To resolve this situation, you must deploy the updated policies on the network devices. Click **Deploy Now** to deploy the changes immediately, or click **Deploy Later** to deploy the changes later.

Cisco ISE provides the runtime policy platform for providing policy download to the network devices on behalf of Catalyst Center. The TrustSec Workcenter user interface screens for Security Groups, Security Group Access Control Lists (SGACLs), and Egress Policy are displayed in Read-Only mode in Cisco ISE to prevent policy synchronization issues.

Delete an access contract

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 In the **Access Contracts** window, check the check box next to the access contract that you want to delete, and then choose whether you want to delete the access contract now or schedule it for later.

You can view the sample contracts in the **Access Contracts** window. You can use or delete those sample contracts. However, you cannot delete the default contracts (Permit IP, Deny IP, Permit_IP_Log, and Deny_IP_Log).

Click the link in the **Policies** column of an access contract to view the policies that use that contract. You cannot delete a contract if it is used in a policy. You must delete the contract from that policy before you delete the contract.

Synchronization of access contracts between Catalyst Center and Cisco ISE

While synchronizing the access contracts in Catalyst Center with Cisco ISE:

- If a contract is present in Catalyst Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a contract is present in Cisco ISE and is not present in Catalyst Center, it is created in Catalyst Center.
- If a contract name is the same in Catalyst Center and Cisco ISE, but the description and traffic rule content are different, Catalyst Center is updated with the data specified in Cisco ISE.
- If the contract name and rule are the same, but the description is different, Catalyst Center is updated with the description specified in Cisco ISE.
- Text SGACL command lines in Cisco ISE are migrated as content that cannot be parsed. You can edit these contracts, but Catalyst Center does not parse them or check the syntax. The changes that you make in Catalyst Center are reflected in Cisco ISE.
- If a policy has multiple SGACLs in Cisco ISE, those contracts are migrated as default policies in Catalyst Center.

An orange triangle icon displays next to an access contract if synchronization with Cisco ISE is incomplete.

The contracts that are learned from ACI are displayed in the **Access Contracts** window with the value **ACI** in the **Created In** column. You cannot edit or delete the access contracts that are learned from ACI, but you can use them in the policies while using the ACI-learned security groups. While creating or updating a policy from the Matrix view, if you select an ACI-learned security group as the destination group, the associated access contracts are displayed in the **Preferred Contracts** tab. You can view all the access contracts in the **All Contracts** tab.

Create group-based access control policy

Security groups and access contracts are the basic building blocks of an access control policy. While creating an access control policy, you can use the security groups and contracts that you have created before, or create new security groups and contracts while creating the policy.

To specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups.

For example, if you want to specify the network resources that can be accessed by the users associated with the *Contractors* source security group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the *Finance Servers* destination security group, you can create an access control policy with a single destination and multiple source groups.

Group-based access control policies can also be created or updated based on the traffic flows for a given source and destination group pair.

Procedure

Step 1 In the **Policy List** or **Matrix** view, click **Create Policies**.

Step 2 To create an access control policy with a single source and multiple destination groups, click **Source to Destination(s)** and complete these steps:

a) Click the radio button next to the source security group that you want to select.

If the security group that you want does not exist, click **Create Security Group** to create a new security group. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.

b) Click **Next**.

c) Choose the destination security groups to map to the selected source security group.

You can view the security group details and edit the security groups, if necessary.



Note If a policy already exists between the source and destination, an orange triangle icon is displayed near a security group.

d) Click **Next**.

e) Click the radio button next to the contract that you want to select. You can view and edit the contract details, if necessary.

If the contract that you want does not exist, click **Create Contract** to create a new contract. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.



Note You can choose only one contract for a policy.

f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected security groups and contract.

g) Choose whether you want to create the policy now or schedule it for later.

Step 3 To create an access control policy with a single destination and multiple source groups, click **Destination to Source(s)** and complete these steps:

a) Click the radio button next to the destination security group that you want to select.

If the security group that you want does not exist, click **Create Security Group** to create a new security group. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.

b) Click **Next**.

c) Choose the source security groups to map to the selected destination security group.

You can view the security group details and edit the security groups, if necessary.

Note If a policy already exists between the source and destination, an orange triangle icon is displayed near a security group.

d) Click **Next**.

e) Click the radio button next to the contract that you want to select.

If the contract that you want does not exist, click **Create Contract** to create a new contract. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.

Note You can choose only one contract for a policy.

f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected security groups and contract.

g) Choose whether you want to create the policy now or schedule it for later.

If the **Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Catalyst Center, see the Cisco Catalyst Center ITSM Integration Guide.

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Policies** window. Click the task status link to view the task details in **Activities > Tasks**. You can edit or cancel a task before it is executed.

Update a group-based access control policy based on traffic flows

Procedure

Step 1 From the policy matrix view, click the cell for which you want to update the group-based access control policy.

Step 2 In the **Policy Details** slide-in pane, click **View Traffic Flows**.

In the **View Traffic Flows** slide-in pane, you can see the rules for the selected contract or the default policy in the left pane. You can view the traffic flows that match any selected rule in the right pane.

Step 3 Click **View Traffic** in the Default Action rule to see the list of flows that match that rule. While modifying an existing policy using access contracts with additional rules, use the **View Traffic** option for any rule to see the list of flows matching that rule.

For policies that are using the Default Action rule (with no explicitly selected access contract), you can select an access contract or create a new access contract to be used by that policy.

For policies with the access contract PERMIT or DENY, you can select an access contract or create a new access contract to be used by that policy.

For policies with the custom access contract, you can edit the selected access contract.

Step 4 After making the required changes, choose one of these options:

- **Save the changes to the existing contract. Changes affect all the policies that reference the contract.**
- **Save the changes as a new contract. Changes are applied only to the current policy.**
- **Save the changes as a new contract. Changes are not applied to any policy.**

Synchronization of policies between Catalyst Center and Cisco ISE

While synchronizing the policies in Catalyst Center with Cisco ISE:

- If a policy is present in Catalyst Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a policy is present in Cisco ISE and is not present in Catalyst Center, it is created in Catalyst Center.
- If a policy contract is different in Cisco ISE, Catalyst Center is updated with the contract specified in Cisco ISE.
- Policy mode information (Enabled, Disabled, or Monitor) is also imported from Cisco ISE.

Cisco ISE has an option to allow multiple SGACLs for a single policy (this option is not enabled by default in Cisco ISE). Catalyst Center does not support the use of multiple access contracts for a single policy. During policy synchronization, if a policy in Cisco ISE has multiple SGACLs, the Catalyst Center administrator is given the option to change that policy to have no contract selected (to use the default policy). The administrator can select a new or existing access contract for that policy after the policy synchronization is complete.

Cisco Group-Based Policy Analytics

About Cisco Group-Based Policy Analytics

Group-Based Policy Analytics enables you with insights to create group-based policies by visualizing communications between assets, to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies.

Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network and their communication to answer these questions:

- Which groups are communicating with each other?
- What kind of communication is this?
- Which group does a given asset belong to?

You can purchase one of these types of licenses for Catalyst Center:

- Essentials
- Advantage
- Premier

The Advantage and Premier licenses contain the Group-Based Policy Analytics package. This package consists of these archives (.tar.gz files):

- Backend
- User Interface
- Summarizer Pipeline
- Aggregation definitions

Install Group-Based Policy Analytics

Cisco Group-Based Policy Analytics is a part of Catalyst Center, but it is not installed by default.

To install Group-Based Policy Analytics:

Procedure

Step 1 From the main menu, choose **System** > **Software Management**.

Step 2 Scroll down to the **Available Applications for 2.3.x.x-xxxxx** area and select **Group-Based Policy Analytics**.

Step 3 Click **Install** to install the application.

Hardware and software compatibility

Platform support

Cisco Group-Based Policy Analytics is supported on these hardware platforms:

- 44 cores, single node or three-node cluster
- 56 cores, single node or three-node cluster
- 112 cores, single node or three-node cluster

These platforms must meet the performance and scalability requirements mentioned here.

For details about the supported hardware, see Cisco UCS M4 appliances or Cisco UCS M5 appliances.

The table lists the performance metrics that Catalyst Center and Cisco Group-Based Policy Analytics support on each of the core platforms. The NetFlow metrics were introduced by Cisco Group-Based Policy Analytics.

Note This table lists the performance metrics for a standalone deployment. These values might vary based on the number of nodes in the cluster and the number of installed packages.

Table 63: Performance metrics

Metric	44 cores, three nodes	56 cores	112 cores
Devices (NADs)	5000 1000 switches or 1000 routers or a combination of both; 4000 APs	8000 2000 switches or 2000 routers or a combination of both; 6000 APs	18,000 5000 switches or 5000 routers or a combination of both; 13,000 APs
Clients (endpoints)	25,000 20,000 wireless; 5,000 wired	40,000 30,000 wireless; 10,000 wired	100,000 60,000 wireless; 40,000 wired
NetFlows per sec	30,000	48,000	120,000

Device support

You must enable NetFlow to use Cisco Group-Based Policy Analytics. This table shows the various ways in which NetFlow can be enabled on different network devices.

Table 64: Device support

Network devices	Series	NetFlow configurable in Telemetry section of Network Settings in Catalyst Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow configurable using the CLI Template tool in the Catalyst Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow collection in fabric deployment	NetFlow collection in nonfabric deployment
Routers	Cisco 1000 Series Integrated Services Routers (ISR1K)	Yes	Yes	Yes	Yes
	Cisco 4000 Series Integrated Services Routers (ISR4K)	Yes	Yes	Yes	Yes
	Cisco Cloud Services Router 1000v Series (CSR 1000v)	Yes	Yes	Yes	Yes
	Cisco 1000 Series Aggregation Services Routers (ASR1K)	Yes	Yes	Yes	Yes

Network devices	Series	NetFlow configurable in Telemetry section of Network Settings in Catalyst Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow configurable using the CLI Template tool in the Catalyst Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow collection in fabric deployment	NetFlow collection in nonfabric deployment
Switches	Cisco Catalyst 9200 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9300 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9400 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9500 Series	No	Yes	Yes	Yes
	Cisco Catalyst 9600 Series	No	Yes	Yes	Yes
	Cisco Catalyst 2k Series	No	Yes	NA	Yes
	Cisco Catalyst 3560 Series	No	Yes	NA	Yes
	Cisco Catalyst 3650 Series	No	Yes	Yes	Yes
	Cisco Catalyst 3850 Series	No	Yes	Yes	Yes
	Cisco Catalyst 4k Series	No	Yes	Yes	Yes
	Cisco Catalyst 6500 Series Switches	No	Yes	Yes	Yes
	Cisco Catalyst 6800 Series Switches	No	Yes	Yes	Yes
Wireless Controllers	Cisco 3504 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 5520 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 8540 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco Catalyst 9800 Based Controller	Yes	Yes	Yes	Yes

Cisco ISE

Catalyst Center supports Cisco ISE 2.4 Patch 7 and later, Cisco ISE 2.6 Patch 1 and later, and Cisco ISE 2.7 and later.

Cisco Stealthwatch

Catalyst Center supports Cisco Stealthwatch 7.x or later.

Understand connectors

Cisco Group-Based Policy Analytics gathers telemetry from various sources, which are also known as connectors. You can configure the connectors either by following the Initial configuration of Cisco Group-Based Policy Analytics, on page 1199 workflow, or by choosing **Policy** > **Group-Based Access Control** > **Analytics** > **Configurations** > **Analytics Settings**.

Group data connectors

The group data connectors collect information about groups that assets are classified into. Cisco ISE and Cisco Stealthwatch are group data connectors.

- **Cisco ISE**

  Cisco ISE is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is installed on a virtual machine, a physical machine, or a combination of both. Cisco ISE uses the Cisco Platform Exchange Grid (pxGrid) service as the publisher-subscriber module for sharing Session Directory, security groups, and other information. PxGrid uses a query interface and supports bulk download. Users on the network are authenticated, authorized, and accounted for, and a Session Directory is maintained. User events are published to the connectors that are subscribed to the Session Directory service. Other services, like security group notifications, can also be subscribed to.

  User identity and device information obtained during authentication is used to classify the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the network so that they can be properly identified for applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the network device to act upon the SGT to filter traffic.

  In addition, Cisco ISE collects information about endpoints connected to your network, such as the type of device, OS, OS version, IP address and other attributes. These are called ISE profiles.

  The Cisco ISE connector provides Cisco Group-Based Policy Analytics with SGT definitions and profiles from Cisco ISE.

- **Cisco Stealthwatch**

  Cisco Stealthwatch is a network-based anomaly detection system that provides advanced threat detection, accelerated threat response, and network traffic security analysis. The Cisco Stealthwatch connector obtains the host groups that are configured on Cisco Stealthwatch. A host group is essentially a virtual container containing multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology.

Communication Connector

The communication connector helps gather information on traffic seen between groups that could be leveraged in group-based policy decisions. This is done using NetFlow from network devices managed by Catalyst Center. NetFlow is collected and aggregated natively by Catalyst Center.

Initial configuration of Cisco Group-Based Policy Analytics

This workflow helps you configure the data connectors that are required to collect telemetry data related to the network activity and endpoints from specific sources, such as Cisco ISE, Cisco Stealthwatch, and NetFlow. This task is useful when you are configuring the data connectors for the first time.

Before you begin

Catalyst Center must have Cisco Group-Based Policy Analytics installed.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Overview**. The **Create policies with more confidence** window displays.

Step 2 Click **Get Started**.
The **Configure your data connectors** window displays.

Step 3 Click **Let's Do It**.

The **Configure Group Data Connectors** window displays.

Note If the Cisco ISE version is earlier than the version required for running Cisco Group-Based Policy Analytics, an error message displays.

Step 4 Click **Configure** at the bottom of the connector that you want to configure.
A new window opens, redirecting you to the Catalyst Center **Settings** window, where you can configure the required connectors. You must configure the Cisco ISE connector. Configuring the Cisco Stealthwatch connector is optional.

Step 5 Close the **Settings** window. A green dot displays next to the **Configure** option for the successfully configured connectors in the **Configure Group Data connectors** window.

Step 6 Click **Next**.
The **Configure Communication Connectors** window displays.

Step 7 Configure the communication connector (NetFlow) by using one of these options:

- Provision NetFlow on the Catalyst Center device interface manually.
- Click **CLI Templates** to configure NetFlow using the **CLI Templates** tool in Catalyst Center.
- Click **Telemetry in Network Settings** to configure NetFlow in the telemetry section of network settings.

Step 8 Click **Next**.
The **Summary** window displays the configuration details of the connectors.

Step 9 Click **Done** to start discovering your groups and endpoints.

Explore groups and endpoints

This section provides information about the different ways to visualize traffic between different groups.

Multiple groups to multiple groups

When you click the number that displays in the **Security Groups** box in the **Overview** window, the **Explore Security Groups** window displays. In this window, you see a summary of all the group-to-group communication among security groups. By default, the time range for this view is the last available 24 hours of data.

Note This is different from the time range mentioned in the **Overview** window, where it is set to the last 14 days. The chart shows the top 25 source security groups and their corresponding interactions, starting with the source security group with the highest number of unique flows within the given time period and so on.

Click the icon to display the chart view or to display the table view.

In the table view, if you click the **See destinations** link on a particular row, it opens a window showing all the destination security groups for the selected source security group and the unique flow count for each destination security group.

Click a source group to view the **Single Group to Multiple Groups** window.

When you hover your cursor over a link, the link is highlighted and a tooltip shows the number of unique traffic flows. Clicking the link takes you to the **Single Group to Single Group** window.

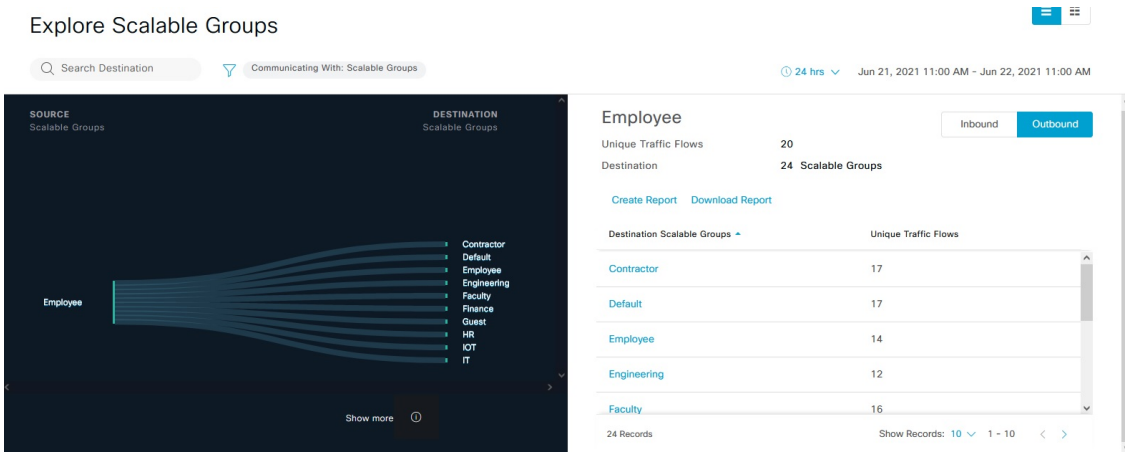
When you click the number displayed in the **ISE Profiles** box in the **Overview** window, the **Explore ISE Profiles** window displays. In this window, you can see a summary of all the communication from ISE Profiles as the source and security groups as the destination. In order to focus on the group-based policy decisions, either the source or destination category must be the security groups in this view.

When you click the number displayed in the **Stealthwatch Host Groups** box in the **Overview** window, the **Explore Stealthwatch Host Groups** window displays. In this window, you can see a summary of all the communication, with Stealthwatch Host Groups as the source and the security groups as the destination. In order to focus on the group-based policy decisions, either the source or destination category must be the security groups in this view.

Single group to multiple groups

Single Group to Multiple Groups: Outbound

This window displays the activity between a single source group and multiple destination groups. The source or the destination or both must be a security group. By default, the time range for this view is the last available 24 hours of data, and the default number of links or records shown is 10.



Click the icon to display the chart view or to view the table view.

Outbound displays the connections initiated by the selected security group. **Inbound** displays the connections initiated by another group to this security group.

Click any column to sort it in ascending or descending order.

Click a group to view the **Single Group to Single Group** window with the corresponding destination as the selected group. The source group does not change.

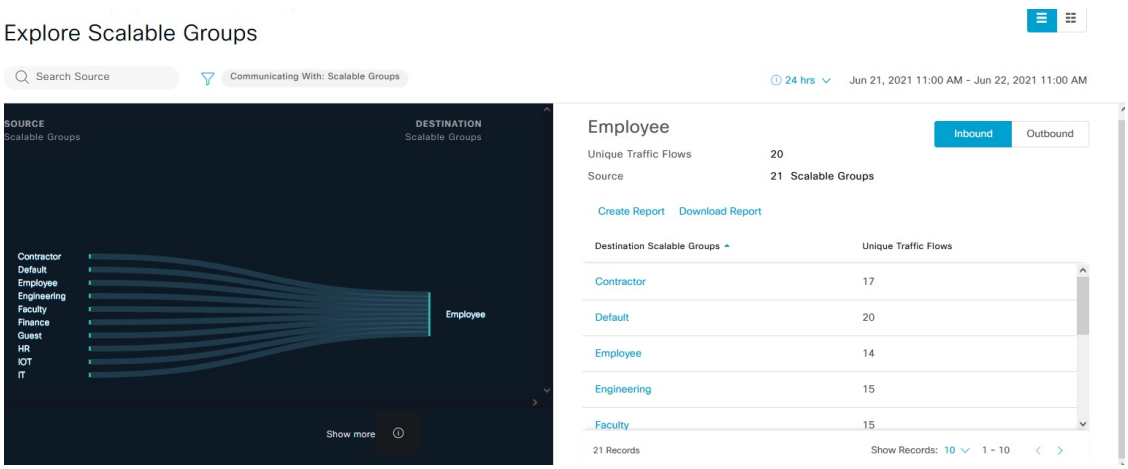
When you hover your cursor over a link, it is highlighted, and a tooltip shows the number of unique traffic flows. If you click this link, it takes you to the **Single Group to Single Group** window.

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

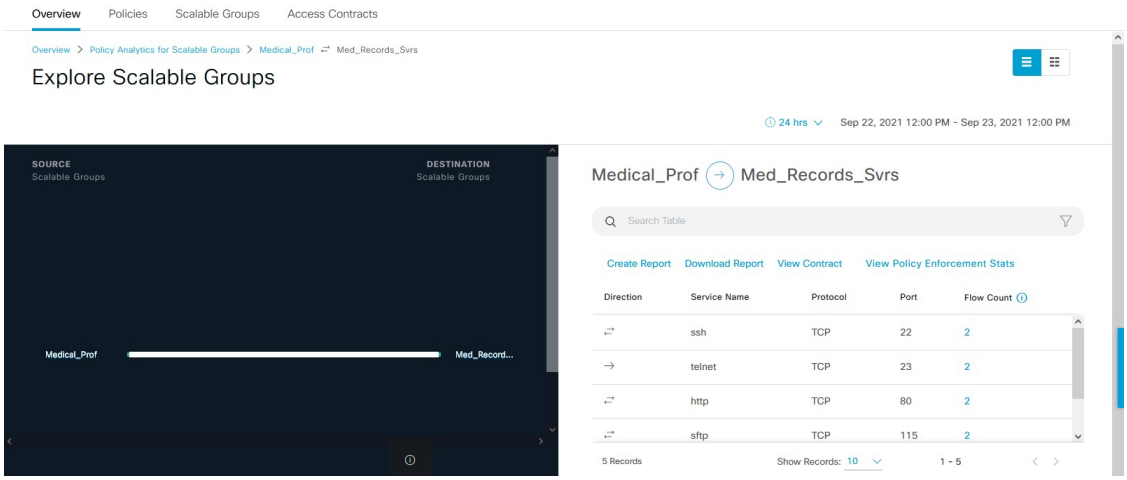
Single Group to Multiple Groups: Inbound

If you click **Inbound**, it shows all the connections initiated by any group as the source and the selected security group as the destination.



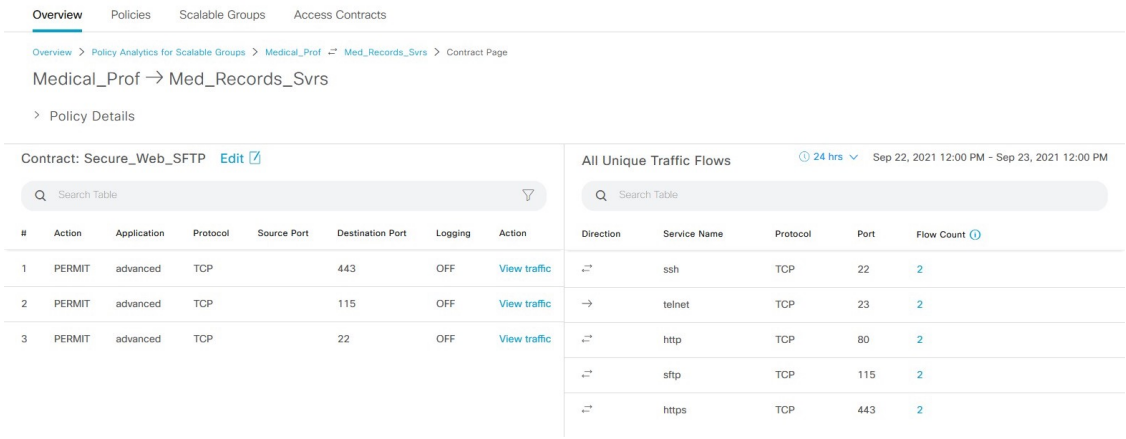
Single group to single group

This window shows the activity between a source group and a destination group. Either the source group, the destination group, or both must be a security group. By default, the time range for this visual is the last available 24 hours of data, and the default number of links or records shown is 10.

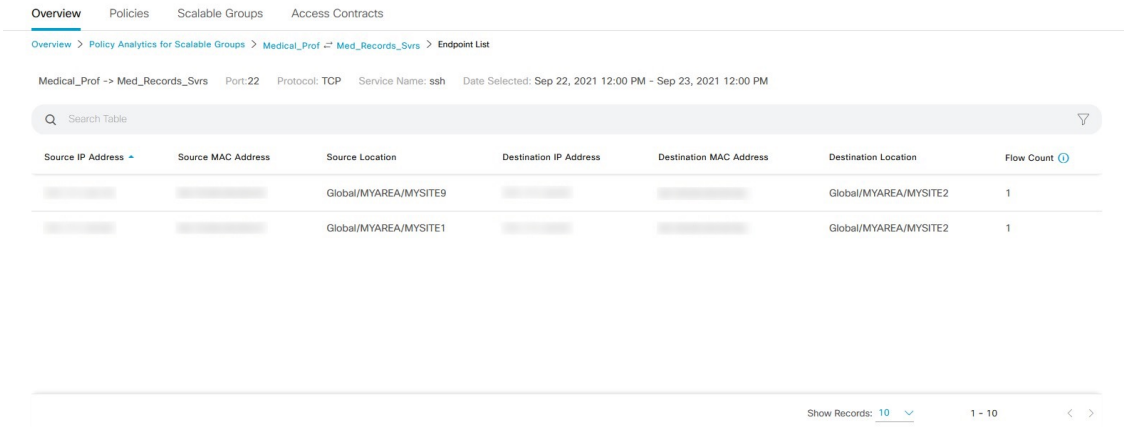


When you click the directional arrow displayed between the source and destination groups, the source and destination groups are interchanged in this view.

Click **View Contract** to view a side-by-side comparison of traffic flows with the access contract rules that are in effect for this source and destination group pair.

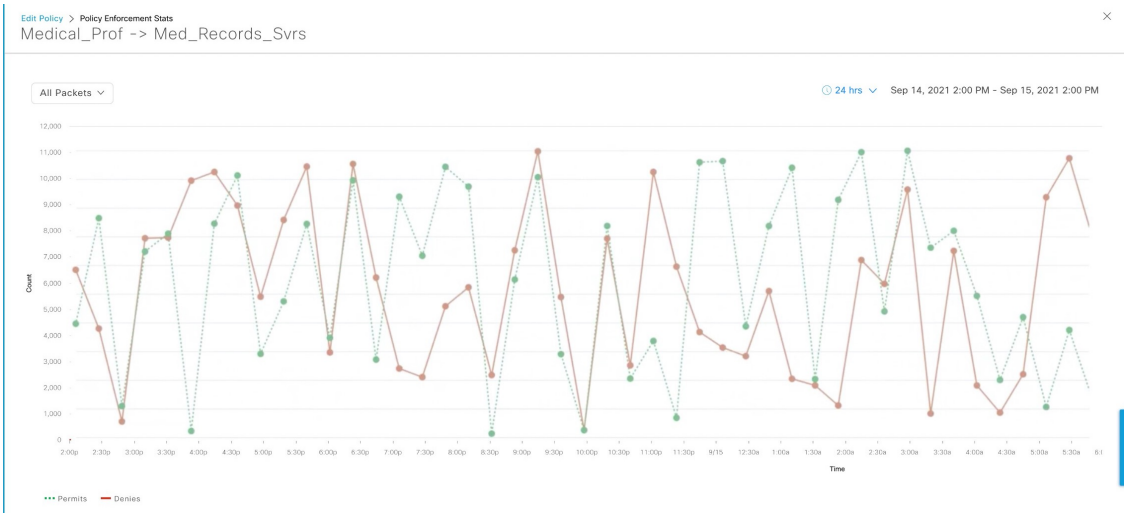


The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane. You can view the flow direction, service name, flow count, ports, and protocol details in the right pane. The **Flow Count** column displays the number of flows detected for that particular service, port, and protocol combination for the selected time period. You can click the flow count link to view the flow details for each endpoint.



Note When you sort the **Traffic Flows** table based on the flow count, only 1000 records display.

Click **View Policy Enforcement Stats** to view a time-series graph of the permit and deny counts for any source and destination group pair. It provides per-policy enforcement statistics visibility. You can use the **All Packets** drop-down list to select only the permitted or dropped packets. Graph data points are displayed for each 15-minute data collection period. You can hover over any data point to view the number of permits and denies. You can click a data point or time period to view the contract and traffic flow details for the selected time period.



Note The selected time period is the hour that contains the 15-minute interval corresponding to the selected data point because the flow data aggregation is done every 60 minutes.

The **Traffic Flows** table can also be accessed from the **Policy Details** slide-in pane while creating or editing a policy.

Click the  icon to display the chart view or  to display the table view.

You can set the date and time using the Date and Time selector.

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

Access contracts

Access contracts can now be created and modified directly in the Analytics workflow.

View a contract

To launch the **View Contract** window, from the **Explore Security Groups** window, click **View Contract**. The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane.

This table can also be accessed from the **Policies** window. From the main menu, choose **Policy** > **Group-Based Access Control** > **Policies**.

From the policy matrix view, click the cell for which you want to create or modify contracts. In the **Policy Details** slide-in pane, click **View Traffic Flows**.

If there is currently no contract assigned between the source and destination groups, no data is displayed. You can use the **Change Contract** or **Create Access Contract** option to create or modify the contract.

Click **View traffic** in the **Action** column to see the list of flows that match that rule.

Create an access contract

To launch the **Contract Content** window, from the **Policy Details** pane, click **Create Access Contract**. To create the traffic filter rules:

1. From the **Action** drop-down list, choose **Deny** or **Permit**.
2. From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

   If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option in the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the + icon and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the Handle icon at the left end of a rule to drag and change the order of the rule.

You can use the **Add to Contract** option within the **All Unique Traffic Flows** pane to add an entry to the contract.

Saving a newly created or edited contract includes these options:

- **Update current policy only**: A duplicate of the contract creates and applies to the current policy. Other policies that reference this contract are not affected.

- **Update contract for all referenced policies**: The contract updates and applies to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract is created but not applied to any policy.

Change a contract

To launch the **Change Contract** window, from the **Policy Details** pane, click **Change Contract**. All the available contracts are displayed. You can select the required contract and click **Change** to add that contract to the policy.

Edit a contract

The **Edit** option displays only when a contract has already been added to the policy. If you want to edit the contract details, click **Edit** next to the name of the contract.

After updating the contract, click **Save**. These options are available:

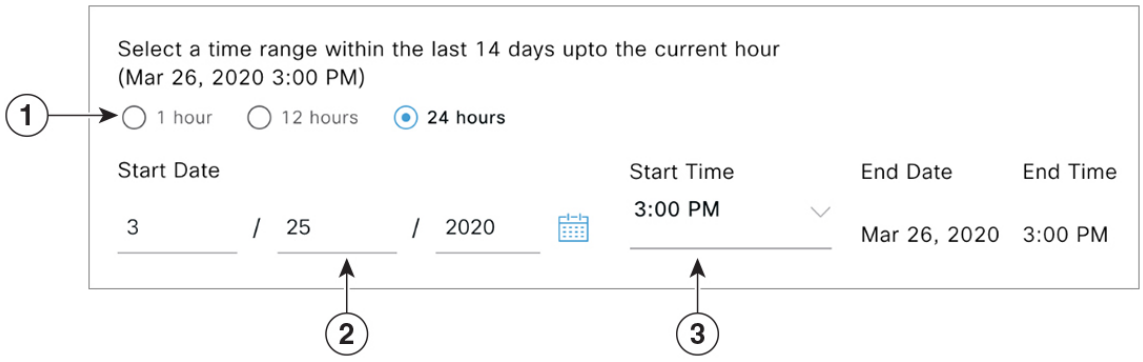
- **Update current policy only**: A duplicate of the contract creates and applies to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies**: The contract updates and applies to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract creates but doesn't apply to any policy.

After choosing the appropriate option, enter a name and description (if you select the first or third option), and then click **Confirm**.

Date and time selector

You can select the time period to specify the data in the connection summary. You can select a time range within the last 14 days up to the current hour.

Figure 31: Date and time selector



1. Select one of the options. The **End Time** adjust automatically.
2. Specify the **Start Date** by entering the month, day, and year manually or by using the calendar icon.

3. Choose the **Start Time** from the drop-down menu.

Use Search

The **Overview** window has a **Search** field that can search across the data for security groups, ISE profiles, Stealthwatch host groups, IP addresses, or MAC addresses.

As you start entering the characters in the search field, an automatic search is performed for security groups, ISE profiles, and Stealthwatch host groups, and up to three results are displayed for each group type. For MAC addresses, the relevant characters are hexadecimal and colon.

Cisco Group-Based Policy Analytics supports both IPv4 and IPv6 addresses for endpoints. You can search and filter the endpoints using an IPv4 or IPv6 address.

- These characters can be used to search and filter IPv4 addresses:
  - Numbers (0-9)
  - Dot (.)

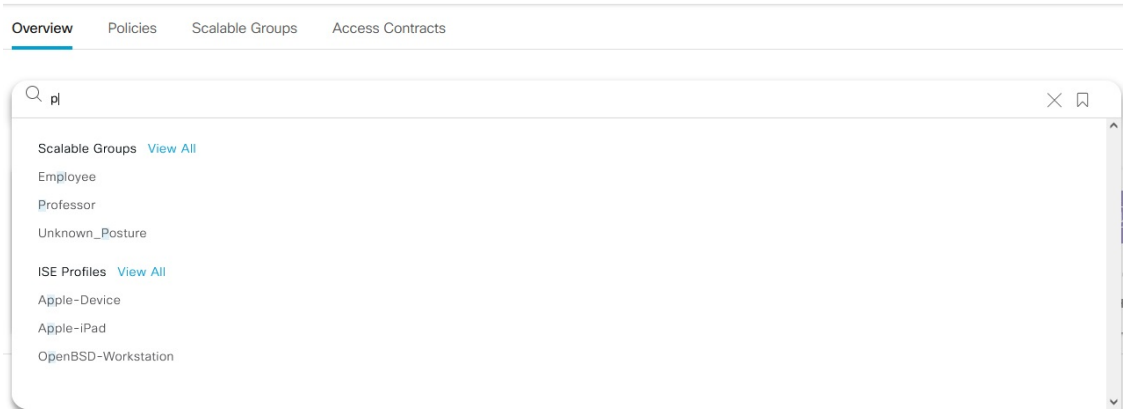
  You can enter up to 15 characters in the filter field.
- These characters can be used to search and filter IPv6 addresses:
  - Numbers (0-9)
  - Lowercase and uppercase alphabetic characters (a-f, A-F)
  - Colon (:)

  You can enter up to 39 characters in the filter field.

Note

- The **Search Results** window does not open until you click the **View All** link.
- A read-only user cannot search for an IP address or a MAC address. For more information, see Role-Based Access Control, on page 1208.

Figure 32: Search window



From the **Focus** drop-down list, choose the required option to change your search criteria.

The filter icon is used in advanced filtering and is available only when you search for a MAC address or an IP address. When you click the filter icon, each column is provided with a search field on top of the column name.

For each column, you can enter up to three search criteria. When entering more than one criterion per column, you can specify an OR operation or an AND operation. The resultant query performs an AND operation across the columns.

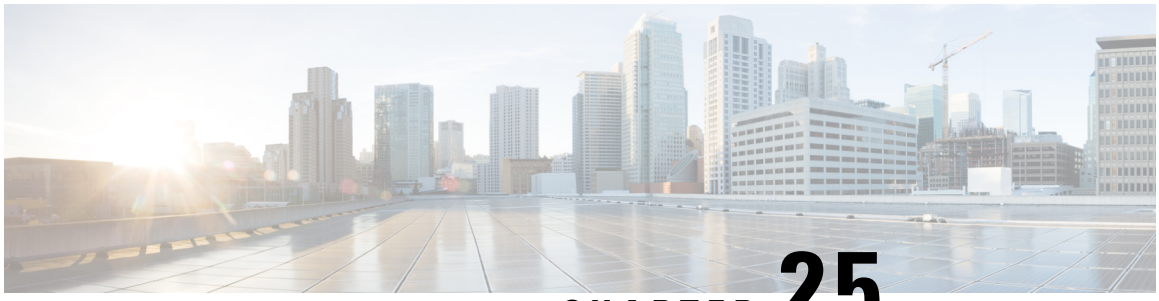
Click the bookmark icon, and use the **Save Current Search** option to save the current displayed search.

To delete a saved search, click the bookmark icon. Hover your cursor over the name of the saved search, and click the cross icon. Click **Yes** in the **Delete Saved Filter** dialog box to permanently delete the filter.

Role-Based Access Control

Cisco Group-Based Policy Analytics supports Role-Based Access Control (RBAC). It differentiates between a read-write user and a read-only user. However, because Cisco Group-Based Policy Analytics is primarily based on visibility, which does not make any changes to the system, there are only a few limitations for a read-only user:

- A read-only user cannot save search queries.
- A read-only user cannot configure the data connectors.
- A read-only user cannot export data because exporting data is an HTTPS POST operation.
- A read-only user can only perform a search by group and is restricted from other search functions because they involve HTTPS POST operations.



CHAPTER 25

Configure IP-Based and URL-Based Access Control Policies

- IP-based access control policies, on page 1209
- Workflow to configure an IP-based access control policy, on page 1210
- Configure global network servers, on page 1210
- Create an IP Network Group, on page 1212
- Edit or delete an IP Network Group, on page 1212
- Create an IP-based access control contract, on page 1212
- Edit or delete an IP-based access control contract, on page 1213
- Create an IP-based and URL-based access control policy, on page 1214
- Edit or delete an IP-based and URL-based access control policy, on page 1215

IP-based access control policies

An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria, including the protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation.

An IP-based access control policy has two main components:

- **IP Network Groups**: IP network groups comprise IP subnets that share the same access control requirements. These groups can be defined only in Catalyst Center. An IP network group may have as few as one IP subnet in it.
- **Access Contract**: An access contract is a common building block that is used in both IP-based and group-based access control policies. It defines the rules that make up the access control policies. These rules specify the actions (permit or deny) done when traffic matches a specific port or protocol and the implicit actions (permit or deny) done when no other rules match.

Workflow to configure an IP-based access control policy

Before you begin

- Cisco ISE is not mandatory if you are adding groups within the **Policy** > **IP & URL Based Access Control** > **IP Network Groups** window while creating a new IP-based access control policy.
- If your browser or network has proxy settings configured, include the proxy subnets in the IP access control policy.
- Make sure that you have defined these global network settings and provision the device:
  - Network servers, such as AAA, DHCP, and DNS servers. For more information, see Configure global network servers, on page 321.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Configure global device credentials, on page 323.
  - IP address pools. For more information, see Configure IP address pools, on page 337.
  - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see Configure global wireless settings, on page 350.

Procedure

Step 1 Create IP network groups.

For more information, see Create an IP Network Group, on page 1212.

Step 2 Create an IP-based access control contract.

An IP-based access control contract defines a set of rules between the source and destination. These rules dictate the action (allow or deny) that network devices perform based on the traffic that matches the specified protocols or ports. For more information, see Create an IP-based access control contract, on page 1212.

Step 3 Create an IP-based access control policy. The access control policy defines the access control contract that governs traffic between the source and destination IP network groups.

For more information, see Create an IP-based and URL-based access control policy, on page 1214.

Configure global network servers

You can define the global network servers that become the default for your entire network.

Note You can override the global network settings on a site by defining site-specific settings.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Servers** tab.

Step 3 Expand the **DHCP** area. Specify one or more dedicated Dynamic Host Configuration Protocol (DHCP) servers for managing the client device networking configuration.

Step 4 Check the **Add DHCP servers** check box to view the fields.

Step 5 In the **IP Address** field, enter the IP address of a DHCP server. Click the icon to add an IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

You must define at least one DHCP server in order to create IP address pools.

Step 6 Expand the **DNS** area to configure your network domain name, and specify Domain Name System (DNS) servers for hostname resolution.

Step 7 Check the **Set a domain name** check box to enter the domain name of a DNS server.

Step 8 Check the **Add DNS servers** check box to enter the IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

You must define at least one DNS server in order to create IP address pools.

Step 9 Expand the **NTP** area to specify one or more Network Time Protocol (NTP) servers to facilitate system clock synchronization for your network.

Step 10 Check the **Add NTP servers** check box to view the fields.

Step 11 In the **IP Address** field, enter the IP address of an NTP server. Click the icon to add an IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

Step 12 Click **Save**.

Create an IP Network Group

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP Network Groups**.
Step 2 Click **Add Groups**.
Step 3 In the **Name** field, enter a name for the IP network group.
Step 4 In the **Description** field, enter a word or phrase that describes the IP network group.
Step 5 In the **IP Address or IP/CIDR** field, enter the IP addresses that make up the IP network group.
Step 6 Click **Save**.

Edit or delete an IP Network Group

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP Network Groups**.
Step 2 In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.
Step 3 Do one of these tasks:

- To edit the group, click **Edit**. For more information about field definitions, see Create an IP Network Group, on page 1212. Make your changes, and click **Save**.
- To delete the group, click **Delete** and then click **Yes** to confirm.

Create an IP-based access control contract

Use this procedure to create an IP-based access contract:

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **Access Contract**.
Step 2 Click **Add Contract**.
Step 3 In the **Name** field of the **Add Contract** slide-in pane, enter a name for the access contract.
Step 4 (Optional) In the **Description** field, enter a description for the access contract.
Step 5 From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.

Step 6 Click **Add** to add a port or protocol.

Step 7 In the **Add Port/Protocol** dialog box, do these steps:

a) From the **Action** drop-down list, choose either **Deny** or **Permit**.
b) From the **Port/Protocol** drop-down list, choose a port or protocol.
c) Click **Save**.

Step 8 If Catalyst Center doesn't have the port or protocol that you need, click **Create Port/Protocol** to create a port and protocol, and do these steps in the **Create Port/Protocol** dialog box:

a) In the **Name** field, enter a name for the port or protocol.
b) From the protocol drop-down list, choose a protocol.
c) In the **Port Range** field, enter the port range.
d) If you want Catalyst Center to configure the port or protocol as defined and not report any conflicts, check the **Ignore Conflict** check box.
e) Click **Save**.

Step 9 (Optional) To include more rules in the access contract, click **Add** and repeat Step 7, on page 1213.

Step 10 Click **Save**.

Edit or delete an IP-based access control contract

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that is deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **Access Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete, and do one of these tasks:

- To make changes to the contract, click **Edit**, make the changes, and click **Save**. For more information about field definitions, see Create an IP-based access control contract, on page 1212.

Note If you make changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.

- To delete the contract, click **Delete**.

Create an IP-based and URL-based access control policy

You can create a post authentication Access Control List (ACL) for your network. The list can be based on IPs, URLs, or both.

Before you begin

See Workflow to configure an IP-based access control policy, on page 1210.

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 Click **Add Policy**.

Alternatively, instead of the first two steps, you can click the menu icon and choose **Workflows** > **Create IP & URL-Based Access Control Policy**. If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 3 In the **Policy Name and Details** window:

a) Enter a name and description for the policy.

b) Under **Select ACL Type**, check the required check boxes:

- **IPv4 or IPv6**: Configure IP-based access control policy.
- **URL**: Configure URL-based access control policy.
- **IPv4** and **URL**: Configure both IPv4-based and URL-based access control policies.
- **IPv6** and **URL**: Configure both IPv6-based and URL-based access control policies.

Step 4 In the **Select Sites and SSID** window, choose the site where you want to apply the policy and select the SSIDs.

Ensure that the site is already provisioned with an SSID.

For Flex or fabric SSIDs, ensure that an AP is provisioned at the site.

If you choose URL ACL, you cannot select local SSIDs along with Flex or fabric SSIDs.

Step 5 If you chose IP ACL, configure custom rules for IP ACL in the **IP Access Control List** window:

If you want to...	Then...
Add a rule	**a.** Click **Add New Rule**. **b.** In the **Add New Rule** dialog box, choose a source, destination, contract, and direction from the corresponding drop-down lists. **Note** For bidirectional rules, ensure that the source and destination are different. Use only custom contracts when the source and destination are set to **Any**. **c.** Click **Add**.

If you want to...	Then...
Edit a rule	**a.** Click the pencil icon for the rule that you want to edit. **b.** Edit the required configuration. **c.** Click **Save**. **Note** You cannot edit the default rule.
Delete a rule	Click the delete icon for the rule that you want to delete. **Note** You cannot delete the default rule.
Update the sequence of a rule	Click the icon for the rule, and drag and drop the rule to the required position. **Note** You cannot update the sequence of the default rule.

Step 6 If you chose URL ACL, do these steps in the **URL Access Control List** window:

a. Enter the URL.

Note You can include up to twenty URLs.

b. From the **Action** drop-down list, choose **Permit** or **Deny**.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Edit or delete an IP-based and URL-based access control policy

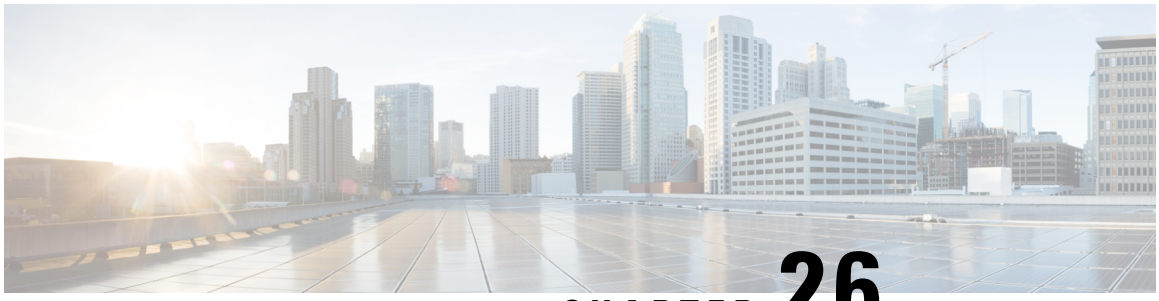
If you need to, you can change or delete an IP-based and URL-based access control policy.

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 To edit a policy, click the name of the policy that you want to edit, make the required changes, and click **Save & Schedule**. For more information, see Create an IP-based and URL-based access control policy, on page 1214.

Step 3 To delete a policy, check the check box next to the policy that you want to delete and click **Delete**.



CHAPTER 26

Configure Application Policies

- Application policies overview, on page 1217
- Manage application policies, on page 1231
- Manage queuing profiles, on page 1241
- Manage application policies for WAN interfaces, on page 1243

Application policies overview

Quality of Service (QoS) refers to the ability of a network to provide preferential or deferential service to selected network traffic. By configuring QoS, you can ensure that network traffic is handled in such a way that makes the most efficient use of network resources while still adhering to the objectives of the business, such as guaranteeing that voice quality meets enterprise standards, or ensuring a high Quality of Experience (QoE) for video.

You can configure QoS in your network using application policies in Catalyst Center. Application policies comprise these basic parameters:

- **Application Sets**: Sets of applications with similar network traffic needs. Each application set is assigned a business relevance group (business relevant, default, or business irrelevant) that defines the priority of its traffic. QoS parameters in each of the three groups are defined based on Cisco Validated Design (CVD). You can modify some of these parameters to more closely align with your objectives.
- **Site Scope**: Sites to which an application policy is applied. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope.

Note For wired devices onboarded through Plug and Play, if you configure QoS policy on a site, the QoS policy is enabled by default on the devices added to the site.

Catalyst Center takes all of these parameters and translates them into the proper device CLI commands. When you deploy the policy, Catalyst Center configures these commands on the devices defined in the site scope.

Note Catalyst Center configures QoS policies on devices based on the QoS feature set available on the device. For more information about a device's QoS implementation, see the corresponding device's product documentation.

CVD-based settings in application policies

The default QoS trust and queuing settings in application policies are based on the Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service Design. CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by Cisco engineers to ensure faster, more reliable, and fully predictable deployment.

The latest validated designs relating to QoS are published in the Cisco Press book, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition, available at: http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694. For additional information, see this Cisco documentation:

- Cisco Validated Designs
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

Site scope

A site scope defines the sites to which an application policy is applied. When defining a policy, you configure whether a policy is for wired or wireless devices. You also configure a site scope. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices in the site scope with the SSID defined in the scope.

This allows you to make tradeoffs as necessary to compensate for differences in the behaviors between wired and wireless network segments. For example, wireless networks typically have lower bandwidth, lower speed, and increased packet loss in comparison to wired networks. Individual wireless segments may exhibit further variation due to local conditions of RF interference, congestion, and other factors, such as the varying capabilities of network devices. The ability to apply per-segment policies to individual wireless segments enables the adjustment of traffic-handling rules to ensure that the highest-priority traffic is least affected by degradation of the wireless network.

Business-relevance groups

A business-relevance group classifies a given application set according to how relevant it is to your business and operations.

Business-relevance groups map to three types of traffic: high priority, neutral, and low priority. These groups include:

- **Business Relevant**: (High-priority traffic) The applications in this group directly contribute to organizational objectives, and as such, may include a variety of applications, including voice, video, streaming, and collaborative multimedia applications, database applications, enterprise resource applications, email, file transfers, content distribution, and so on. Applications designated as business relevant are treated according to industry best-practice recommendations, as prescribed in Internet Engineering Task Force (IETF) RFC 4594.
- **Default**: (Neutral traffic) This group is intended for applications that may or may not be business relevant, for example, generic HTTP or HTTPS traffic may contribute to organizational objectives at times, while at other times, such traffic may not. You may not have insight into the purpose of some applications, for instance, legacy applications or even newly deployed applications. Therefore, the traffic flows for these applications should be treated with the Default Forwarding service, as described in IETF RFC 2747 and 4594.
- **Business Irrelevant**: (Low-priority traffic) This group is intended for applications that have been identified as having no contribution towards achieving organizational objectives. They are primarily consumer-oriented or entertainment-oriented or both in nature. We recommend that this type of traffic be treated as a *Scavenger* service, as described in IETF RFCs 3662 and 4594.

Applications are grouped into application sets and sorted into business-relevance groups. You can include an application set in a policy as-is, or you can modify it to meet the needs of your business objectives and your network configuration.

For example, YouTube is a member of the consumer-media application set, which is business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies, for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can move the YouTube application into the streaming-video application set, which is business relevant by default.

Consumers and producers

You can configure relationships between applications such that when traffic from one application is sent to another application (thus creating a specific a-to-b traffic flow), the traffic is handled in a specific way. The applications in this relationship are called *producers* and *consumers*, and are defined as:

- **Producer**: Sender of the application traffic. For example, in a client/server architecture, the application server is considered the producer because the traffic primarily flows in the server-to-client direction. In the case of a peer-to-peer application, the remote peer is considered the producer.
- **Consumer**: Receiver of the application traffic. The consumer may be a client endpoint in a client/server architecture or it may be the local device in a peer-to-peer application. Consumers may be endpoint devices, but may, at times, be specific users of such devices (typically identified by IP addresses or specific subnets). There may also be times when an application is the consumer of another application's traffic flows.

Setting up this relationship allows you to configure specific service levels for traffic that matches this scenario.

Marking, queuing, and dropping treatments

Catalyst Center bases its marking, queuing, and dropping treatments on IETF RFC 4594 and the business relevance category that you have assigned to the application. Catalyst Center assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant

Business category to the Scavenger application class. For applications in the Relevant Business category, Catalyst Center assigns traffic classes to applications based on the type of application. This table lists the application classes and their treatments.

Table 65: Marking, queuing, and dropping treatments

Business relevance	Application class	Per-hop behavior	Queuing and dropping	Application description
Relevant	VoIP[5]	Expedited Forwarding (EF)	Priority Queuing (PQ)	VoIP telephony (bearer-only) traffic; for example, Cisco IP phones.
	Broadcast Video	Class Selector (CS) 5	PQ	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows; for example, Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows are flows that are highly drop sensitive and have no retransmission or flow-control capabilities or both.)
	Real-time Interactive	CS4	PQ	Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco TelePresence.
	Multimedia Conferencing	Assured Forwarding (AF) 41	Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)	Desktop software multimedia collaboration applications and audio and video components of these applications; for example, Cisco Jabber and Cisco Webex.
	Multimedia Streaming	AF31	BW Queue and DSCP WRED	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications, such as Cisco Digital Media System.
	Network Control	CS6	BW Queue only[6]	Network control-plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.
	Signaling	CS3	BW Queue and DSCP	Control-plane traffic for the IP voice and video telephony infrastructure.
	Operations, Administration, and Management (OAM)	CS2	BW Queue and DSCP[7]	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP WRED	Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP WRED	Noninteractive (background) data applications, such as email, file transfer protocol (FTP), and backup applications.

Business relevance	Application class	Per-hop behavior	Queuing and dropping	Application description
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small number of applications are assigned to priority, guaranteed bandwidth, or even to differential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) and DSCP	Nonbusiness related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

[5] VoIP signaling traffic is assigned to the Call Signaling class.
[6] WRED is not be enabled on this class because network control traffic should not be dropped.
[7] WRED is not enabled on this class because OAM traffic should not be dropped.

Service provider profiles

Service provider profiles define the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class models.

When application policies are deployed on the devices, each service provider profile is assigned a certain service-level agreement (SLA) that maps each service provider class to a DSCP value and a percentage of bandwidth allocation.

You can customize the DSCP values and the percentage of bandwidth allocation in a service provider profile when configuring an application policy.

After you create the service provider profile, you need to configure it on the WAN interfaces.

Table 66: Default SLA attributes for service provider profiles with four classes

Class Name	DSCP	Priority class	SLA	
			Bandwidth (%)	Remaining bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Default	0	—	—	31

Table 67: Default SLA attributes for service provider profiles with five classes

Class Name	DSCP	Priority class	SLA	
			Bandwidth (%)	Remaining bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Class 3 Data	AF11	—	—	1
Default	Best Effort	—	—	30

Table 68: Default SLA attributes for service provider profiles with six classes

Class Name	DSCP	Priority class	SLA	
			Bandwidth (%)	Remaining bandwidth (%)
Class 1 Data	AF31	—	—	10
Class 3 Data	AF11	—	—	1
Video	AF41	—	—	34
Voice	EF	Yes	10	—
Default	0	—	—	30
Class 2 Data	AF21	—	—	25

Table 69: Default SLA attributes for service provider profiles with eight classes

Class Name	DSCP	Priority class	SLA	
			Bandwidth (%)	Remaining bandwidth (%)
Network-Control Management	CS6	—	—	5
Streaming Video	AF31	—	—	10
Call Signaling	CS3	—	—	4
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—
Default	0	—	—	25

Class Name	DSCP	Priority class	SLA	
			Bandwidth (%)	Remaining bandwidth (%)
Critical Data	AF21	—	—	25

Queuing profiles

Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.

Note Queuing profiles do not apply to WAN-facing interfaces that are connected to a service provider profile.

These interface speeds are supported:

- 100 Gbps
- 10/40 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

If the speed of an interface falls between two interface speeds, Catalyst Center treats the interface at the lower interface speed.

Note Catalyst Center attempts to detect the operational speed of the interface in order to apply the correct policy. However, if a switch port is administratively down, Catalyst Center cannot detect the speed. In this case, Catalyst Center uses the interface's supported speed.

You define a queuing policy as part of an application policy. When you deploy the application policy, the devices in the sites that are selected in the site scope are configured with the assigned LAN queuing policy. If no LAN queuing policy is assigned, the application policy uses the default CVD queuing policy.

If you change the queuing policy in an application policy that has already been deployed, the policy becomes stale, and you need to redeploy the policy for the changes to be configured on the devices.

Note Additional guidelines and limitations of queuing policies include:

- You cannot delete a LAN queuing profile if it is used in a policy.
- If you update a queuing profile that is associated with a policy, the policy is marked as stale. You need to redeploy the policy to provision the latest changes.
- Traffic class queuing customization does not affect interfaces on Cisco service provider switches and routers. You should continue to configure these interfaces without using Catalyst Center.

Table 70: Default CVD LAN queuing policy

Traffic class	Default bandwidth (Total = 100%)[8]
Business Relevant Voice	10%
Business Relevant Broadcast Video	10%
Business Relevant Real-Time Interactive	13%
Business Relevant Multimedia Conferencing	10%
Business Relevant Multimedia Streaming	10%
Business Relevant Network control	3%
Business Relevant Signaling	2%
Business Relevant OAM	2%
Business Relevant Transactional Data	10%
Business Relevant Bulk Data	4%
Business Relevant Scavenger	1%
Business Relevant Best Effort	25%

[8] We recommend that the total bandwidth for Voice, Broadcast Video, and Real-Time Interactive traffic classes equals no more than 33%.

Processing order for devices with limited resources

Some network devices have a limited memory (called TCAM) for storing network ACLs and access control entries (ACEs). So, because ACLs and ACEs for applications are configured on these devices, the available TCAM space is used. When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

To ensure that QoS policies for the most important applications get configured on these devices, Catalyst Center allocates TCAM space in this order:

1. **Rank**: Number assigned to custom and favorite applications, but not to existing, default NBAR applications. The lower the rank number, the higher the priority. For example, an application with rank 1 has a higher priority than an application with rank 2, and so on. Having no rank is the lowest priority.

Note
- Custom applications are assigned rank 1 by default.
- If we mark the NBAR application as favorite, the rank is set to 1000.

2. **Traffic Class**: Priority based on this order: Signaling, Bulk Data, Network Control, Operations Administration Management (Ops Admin Mgmt), Transactional Data, Scavenger, Multimedia Streaming, Multimedia Conferencing, Real Time Interactive, Broadcast Video, and VoIP Telephony.
3. **Popularity**: Number (1–10) that is based on CVD criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.

Note
- Custom applications are assigned popularity 0.
- Default NBAR applications are assigned a popularity number (1–10) that is based on CVD criteria. When you mark an application as a favorite, this does not change the popularity number; only the rank is changed.

4. **Alphabetization**: If two or more applications have the same rank and popularity number, they are sorted alphabetically by the application's name, and assigned a priority accordingly.

For example, let us assume that you define a policy that has these applications:

- Custom application, custom_realtime, which has been assigned rank 1 and popularity 10 by default.
- Custom application, custom_salesforce, which has been assigned rank 1 and popularity 10 by default.
- Application named corba-iiop, which is in the transactional data traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 9 (based on CVD).
- Application named gss-http, which is in the Ops Admin Mgmt traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 10 (based on CVD).
- All other, default NBAR applications, which have no rank, but will be processed according to their traffic class and default popularity (based on CVD).

According to the prioritization rules, the applications are configured on the device in this order:

Application configuration order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	

Application configuration order	Reason
3. Favorite application, gss-http	Because both of these applications have been designated as favorites, they have the same application ranking. So, Catalyst Center evaluates them according to their traffic class. Because gss-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Transactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.
4. Favorite application, corba-iiop	
5. All other, default NBAR applications	All other applications are next and are prioritized according to traffic class and then popularity, with the applications having the same popularity being alphabetized according to the application's name.

Policy drafts

When you create a policy, you can save it as a draft without having to deploy it. Saving it as a draft allows you to open the policy later and make changes to it. You can also make changes to a deployed policy, and save it as a draft.

Note After you save or deploy a policy, you cannot change its name.

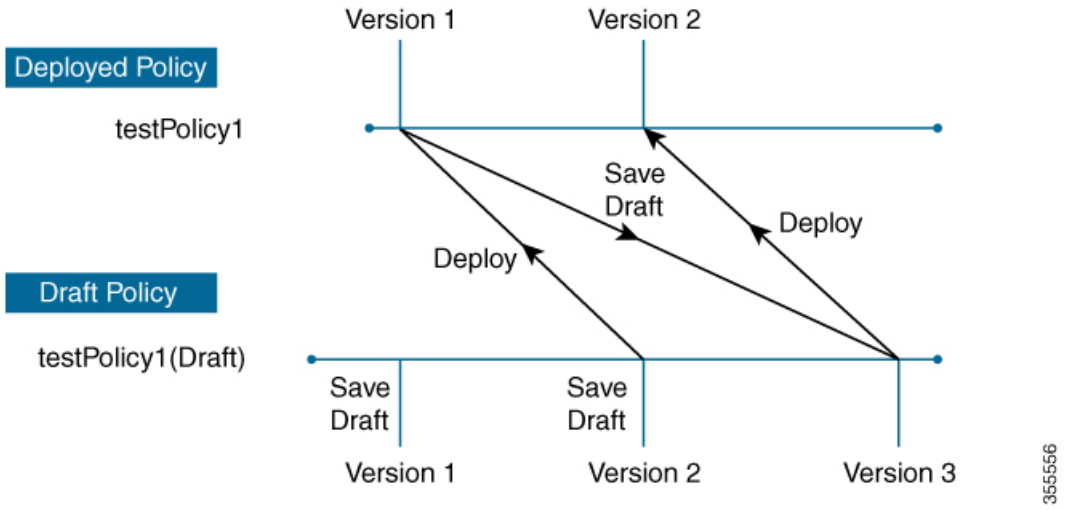
Draft policies and deployed policies are related to one another, but they have their own versioning.

When you save a policy as a draft, Catalyst Center appends the policy name with (Draft), and increments the version number. When you deploy a policy, Catalyst Center increments the version number of the deployed policy.

For example, as shown in the figure, you create a policy named testPolicy1 and save it as a draft. The policy is saved as testPolicy1 (Draft), version number 1. You make a change to the draft and save it again. The policy has the same name, testPolicy1 (Draft), but its version number is incremented to 2.

You decide you like the policy, and you deploy it to the network. The policy is deployed with the name testPolicy1 and its version number is 1. You make a change to the deployed policy and save it as a draft. The draft policy, testPolicy1 (Draft), is incremented to version number 3. When you ultimately deploy that version, testPolicy1 is incremented to version 2.

Figure 33: Deployed policy and draft policy versioning



Any time you modify and save either a draft policy or a deployed policy, the draft policy version number is incremented. Similarly, any time you deploy either a draft policy or a modified deployed policy, the deployed policy version is incremented.

Just as with deployed policies, you can display the history of draft policies and roll them back to previous versions.

For more information about viewing the history of policy versions and rolling back to a previous version, see Policy Versioning, on page 1228.

Policy scheduling

After you create or change a policy, you can deploy or redeploy the policy to the devices associated with it. You can deploy or redeploy a policy immediately or at a specific date and time, for example, on a weekend during off-peak hours. You can schedule a policy deployment for wired or wireless devices.

After you have scheduled a policy to be deployed, the policy and site scope are locked. You can view the policy, but you cannot edit it. If you change your mind about deploying the policy, you can cancel it.

Note When the scheduled event occurs, the policy is validated against the various policy components, for example, applications, application sets, and queuing profiles. If this validation fails, the policy changes are lost.

Policy Versioning

Policy versioning allows you to do these tasks:

- Compare a previous version to the current (latest) one to see the differences.
- Display previous versions of a policy and select a version to reapply to the devices in a site scope.

Editing one version of a policy does not affect other versions of that policy or the components of the policy, such as the application sets that the policy manages. For example, deleting an application set from a policy does not delete the application set from Catalyst Center, other versions of that policy, or even other policies. Because policies and application sets exist independent of each other, it is possible to have a policy version that contains application sets that no longer exist. If you attempt to deploy or roll back to an older version of a policy that references an application set that no longer exists, an error occurs.



Note Policy versioning does not capture changes to applications (such as rank, port, and protocol), application set members, LAN queuing profiles, and sites.

Original policy restore

The first time that you deploy a policy to devices, Catalyst Center detaches the device's original Cisco Modular QoS CLI policy configurations, but leaves them on the device. Catalyst Center stores the device's original NBAR configurations in Catalyst Center. This allows you to restore the original Modular QoS CLI policies and NBAR configuration onto the devices later, if needed.



Note Because the Modular QoS CLI policies are not deleted from the device, if you remove these policies, you will not be able to restore them using the Catalyst Center original policy restore feature.

When you restore the original policy configuration onto a device, Catalyst Center removes the existing policy configuration that you deployed and reverts to the original configuration that was on the device.

Any Modular QoS CLI policy configurations that existed before you deployed application policies are reattached to the interfaces. However, queuing policies, such as multilayer switching (MLS) configurations, are not restored; instead, the devices retain the MLS configurations that were last applied through Catalyst Center.

After you restore the original policy configuration to the device, the policy that is stored in Catalyst Center is deleted.



Note Additional guidelines and limitations for this feature include:

- If the first attempt to deploy a policy to a device fails, Catalyst Center automatically attempts to restore the original policy configurations onto the devices.
- If a device is removed from an application policy after that policy has been applied to the device, the policy remains on the device. Catalyst Center does not automatically delete the policy or restore the QoS configuration on the device to its original (pre-Catalyst Center) configuration.

Stale application policies

An application policy can become stale if you change the configuration of something that is referenced in the policy. If an application policy becomes stale, you need to redeploy it for the changes to take affect.

An application policy can become stale for any of these reasons:

- Change to applications referenced in an application set.
- Change to interfaces, such as service provider profile assignment, WAN subline rate, or WAN or LAN marking.
- Change to the queuing profile.
- New site added under a parent site in the policy.
- Device added to a site that is referenced by the policy.
- Devices moved between sites in the same policy.
- Change in interfaces exclusion/inclusion.
- Change in device Controller-Based Application Recognition (CBAR) status.

Application policy guidelines and limitations

- Catalyst Center cannot learn multiple WLANs with the same SSID name on a wireless controller. At any point, Catalyst Center has only one entry for a WLAN with a unique name, although it is possible for the Cisco Wireless Controller to contain multiple entries with the same name and different WLAN profile names.

  You might have duplicate SSID names per wireless controller by design, or you might have inadvertently added a wireless controller with a duplicate SSID name using Catalyst Center. In either case, having duplicate SSID names per wireless controller is problematic for several features:

  - **Learn Config**: Catalyst Center learns only one randomly chosen SSID name per wireless controller and discards any remaining duplicate SSID names. (**Learn Config** is typically used in existing deployment scenario.)
  - **Application policy**: When deploying an application policy, Catalyst Center randomly applies the policy to only one of the duplicate SSID names and not the others. In addition, policy restore, CLI preview, EasyQoS Fastlane, and PSK override features either fail or have unexpected outcomes.
  - **Multiscale network**: In a multiscale network, multiple duplicate SSID names on multiple devices can cause issues. For example, one device has a WLAN configured as a nonfabric SSID, and a second device has the same WLAN, but it is configured as a fabric SSID. When you do a **Learn Config**, only one SSID name is learned. The other SSID name from the other device is discarded. This behavior can cause conflicts, especially if the second device supports only fabric SSID names, but Catalyst Center is trying to do operations on the device with nonfabric SSID names.
  - **IPACL policy**: When deploying an IPACL policy, Catalyst Center randomly applies the policy to only one of the duplicate SSIDs. In addition, scenarios involving Flex Connect are also impacted.

- Catalyst Center does not recommend out-of-band (OOB) changes to device configurations. If you make OOB changes, the policy in Catalyst Center and the one configured on the device become inconsistent. The two policies remain inconsistent until you deploy the policy from Catalyst Center to the device again.
- The QoS trust functionality cannot be changed.
- Make sure you delete the corresponding wireless application policy before deleting an SSID from design and reprovisioning the wireless controller.

- Wireless application for Cisco Catalyst 9800 Series Wireless Controller is not supported on SSID provisioned through learned configuration.
- Catalyst Center provides ACL-based Application Policy support for Cisco Catalyst IE 3300 Rugged Series switches and Cisco Catalyst IE 3400 Heavy Duty Series switches. You can deploy a maximum of eight port-based custom applications. However, there is no restriction for DSCP-based applications.
- For wireless, you can select only one SSID at a time to deploy the QoS policy. For QoS deployment on multiple SSIDs, keep deploying the policy on SSIDs one after the other.
- For wireless, Catalyst Center pushes only the Marking policy.
- Before starting to use Application Policy for wireless, make sure the wireless controller and the AP are provisioned using Catalyst Center.



Note Catalyst Center does not support FlexConnect Local Switching mode for AireOS and Catalyst 9800 Series Wireless Controller platforms.

Manage application policies

These sections provide information about how to manage application policies.

Prerequisites

To configure application policies, you must address these requirements:

- Catalyst Center supports most Cisco LAN, WAN, and WLAN devices. To verify whether the devices and software versions in your network are supported, see the *Cisco Catalyst Center Compatibility Matrix*.
- Make sure that your Cisco network devices, such as the ISR-G2, ASR 1000, and wireless controller, have the Application Visibility and Control (AVC) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ*.
- AVC support is available for switches running Cisco IOS-XE 16.9 only if auto-QoS is not configured on the switches. You must upgrade the switches with auto-QOS to Cisco IOS-XE 16.11 or later to get AVC support.
- For Catalyst Center to identify the WAN interfaces that need policies, you must specify the interface type (WAN), and optionally, its subline rate and service-provider Class-of-Service model. For more information, see Assign a service provider profile to a WAN interface, on page 1244.
- Verify that the device roles that were assigned to devices during the discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see Change the device role manually, on page 180.

Create an application policy

This section provides information about how to create an application policy.

Before you begin

- Define your business objectives. For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize nonbusiness applications. Based on these objectives, decide which business relevance category your applications fall into.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.
- Verify that the device roles that were assigned to devices during the discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see Change the device role manually, on page 180.
- Add devices to sites. For more information, see Assign an unprovisioned device to a site, on page 156.
- If you plan to configure this policy with a service provider profile for traffic that is destined for a service provider, make sure that you have configured a service provider profile. After creating the application policy, you can return to the service provider profile and customize its SLA attributes and assign the service provider profile to WAN interfaces. For more information, see Configure service provider profiles, on page 350.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Application QoS Policy Name** field, enter a name for the policy.

Step 4 Click either the **Wired** or **Wireless** radio button.

Step 5 For wireless networks, select an SSID that is provisioned from the **SSID** drop-down list.

Step 6 Click **Site Scope**.

Step 7 Click **Edit Site Scope** and check the check box next to the sites where you want to deploy the policy.

Note For policies of wired devices, you cannot select a site that is already assigned to another policy. For policies of wireless devices, you cannot select a site that is already assigned to another policy with the same SSID.

For wired devices onboarded through Plug and Play, if QoS policy is configured on a site, the QoS policy is enabled by default on the devices added to the site.

Step 8 For policies of wired devices, you can exclude devices or specific interfaces from being configured with the policy:

a) From the **Site Scope** pane, click the ellipsis icon (***) next to the site you are interested in.

A list of devices in the selected scope displays.

b) Locate the device that you want to exclude and click the toggle button in the corresponding **Policy Exclusions** column.

c) To exclude specific interfaces, click **Exclude Interfaces**.

d) From the list of **Applicable Interfaces**, click the toggle button next to the interfaces that you want to exclude.

By default, only the **Applicable Interfaces** are shown. You can choose **All** from the **Show** drop-down list to view all the interfaces.

e) Click < **Back to Devices in *Site-Name***.
f) Click < **Back to Site Scope**.

Step 9 For WAN devices, you can configure specific interfaces:

a) From the **Site Scope** pane, click the ellipsis icon ••• next to the desired site.
b) From the list of devices in the site, click **Configure** in the **SP Profile Settings** column next to the desired device.

Note This option is only available for routers.

c) In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.
d) In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:

- Physical interface: Choose **WAN**. This role is the only valid role for a physical interface.
- Tunnel interface: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

e) In the **Service Provider Profile** column, from the **Select Profile** drop-down list, choose a service provider profile.
f) (Optional) If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
g) (Optional) To configure additional WAN interfaces, click + and repeat Step c through Step f.
h) Click **Save**.
i) Click < **Back to Site Scope**.

Step 10 From the **Site Scope** pane, click **OK**.

Step 11 (Optional) If the CVD queuing profile (CVD_QUEUING_PROFILE) does not meet your needs, create a custom queuing profile.

a) Click **Queuing Profiles**.
b) Select a queuing profile from the list in the left pane.
c) Click **Select**.

Step 12 (Optional) If this policy is for traffic that is destined for a service provider, customize the service provider profile SLA attributes:

a) Click **SP Profile**.
b) Choose a service provider profile.
c) Customize the SLA attributes (**DSCP**, **SP Bandwidth %**, and **Queuing Bandwidth %**).

Step 13 (Optional) Configure the business relevance of the application sets used in your network.

Catalyst Center comes with application sets that are preconfigured into business-relevancy groups. You can keep this configuration or modify it by dragging and dropping an application set from one business-relevancy group to another.

Applications marked as a favorites are listed at the top of the application set. To change favorites, go to the Applications registry.

Step 14 (Optional) Customize applications by creating consumers and assigning them to applications, or by marking an application as bidirectional:

a) Expand the application group.

b) Click the gear icon next to the desired application.

c) From the **Traffic Direction** area, click the **Unidirectional** or **Bi-directional** radio button.

d) To choose an existing consumer, from the **Consumer** drop-down list, choose the consumer that you want to configure. To create a new consumer, click **+ Add Consumer** and define the **Consumer Name**, **IP/Subnet**, **Protocol**, and **Port/Range**.

e) Click **OK**.

Step 15 Configure host tracking. Click the **Host Tracking** toggle button to turn host tracking on or off.

When deploying an application policy, Catalyst Center automatically applies ACL entries to the switches to which collaboration endpoints (such as Telepresence units or Cisco phones) are connected.

The ACE matches the voice and video traffic generated by the collaboration endpoint, ensuring that the voice and video traffic are correctly marked.

When host tracking is turned on, Catalyst Center tracks the connectivity of the collaboration endpoints within the site scope and to automatically reconfigure the ACL entries when the collaboration endpoints connect to the network or move from one interface to another.

When host tracking is turned off, Catalyst Center does not automatically deploy policies to the devices when a collaboration endpoint moves or connects to a new interface. Instead, you need to redeploy the policy for the ACLs to be configured correctly for the collaboration endpoints.

Step 16 Do one of these tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy drafts, on page 1227.
- Deploy the policy by clicking **Deploy**.

  Depending on Visibility and Control of Configurations settings, you can either:

  - Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
  - Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

View application policy information

You can display various information about the application policies that you have created and deployed.

Before you begin

You must have at least one deployed application policy.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Sort the policies by name, or filter them by name, status, or queuing profile.

Step 3 View the list of policies and the information about each, including:

- **Policy Name**: Name of the policy.
- **Version**: Iteration of the policy. Each time a policy is deployed or saved as a draft, it is incremented by one version. For example, when you create a policy and deploy it, the policy is at version 1. If you change the policy and deploy it again, the version of the policy is incremented to version 2. For more information, see Policy drafts, on page 1227 and Policy Versioning, on page 1228.
- **Policy Status**: State of the policy. If the policy applied on Cisco Catalyst 3850, Catalyst 4500, and Catalyst 9000 devices and is impacted by the port channel update (create/modify/delete), an alert is shown in the policy status.
- **Deployment Status**: State of the last deployment (per device). Presents a summary, including:
  - Devices that were successfully provisioned.
  - Devices that failed to be provisioned.
  - Devices that were not provisioned due to the deployment being ended.

  Clicking the state of the last deployment displays the Policy Deployment window, which provides a filterable list of devices on which the policy is deployed. For each device, information displays, including:
  - Device details (name, site, type, role, and IP address)
  - Success deployment status. Clicking the gear icon next to the status launches the **Effective Marking Policy** window that shows the **Business Relevant** and **Business Irrelevant** applications and the traffic class queue in which they end up. For devices that have limited TCAM resources or an old NBAR protocol pack, only a subset of the applications that are included in the policy can be provisioned, and they are shown in the view.
  - Failure status shows the reason for the failure.
- **Scope**: Number of sites (not devices) that are assigned to the policy. For policies of wireless devices, the name of the SSID to which the policy applies is included.
- **LAN Queuing Profile**: Name of the LAN queuing profile that is assigned to the policy.

Edit an application policy

You can edit an application policy.

Before you begin

You must have created at least one policy.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to edit.

Step 3 Click the radio button next to corresponding policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Make changes to the application policy, as needed.

Step 6 You can change the business relevance of an application by moving application set between business relevant, business irrelevant, and default groups.

For information about the application policy settings, see Create an application policy, on page 1231.

Step 7 To update the queuing profile, click **Queuing Profiles**, and select a queuing profile from the list in the left pane.

Step 8 Click **Select**.

Step 9 Do one of these tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy drafts, on page 1227.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Run Now** radio button and click **Apply**.

  To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see Policy scheduling, on page 1228.

Note The site time zone setting is not supported for scheduling application policy deployments.

Save a draft of an application policy

When creating, editing, or cloning a policy, you can save it as a draft so that you can continue to modify it later. You can also make changes to a deployed policy and save it as a draft.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Create, edit, or clone a policy.

Step 3 Click **Save Draft**.

For more information, see Policy drafts, on page 1227.

Deploy an application policy

If you make changes that affect a policy's configuration, such as adding a new application or marking an application as a favorite, you must redeploy the policy to implement these changes.

Note Before deploying a policy, the Auto-QoS configuration is removed automatically from Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 devices with Cisco IOS 16.x or later.

After creating custom applications, if CBAR is enabled for a device, the custom applications are configured automatically on the device. You must wait for the synchronization to the latest application registry to complete before deploying the application policy on the device. You can view the synchronization status in **Provision** > **Services** > **Service Catalog** > **Application Visibility**.

If CBAR is enabled for a device, while deploying the application policy, only the attribute sets and maps are configured on the device, because the custom applications are configured through CBAR.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to deploy.

Step 3 Click the radio button next to the policy that you want to deploy.

Step 4 From the **Actions** drop-down list, choose **Deploy**.

a) If you redeploy the policy, you are prompted to take an appropriate action for the devices that were removed from the policy scope. Choose any one of these actions:

- Delete policy from the devices (recommended)
- Remove devices from policy scope
- Remove devices from policy scope and restore devices to the existing configuration

b) Click **Apply**.

Step 5 You are prompted to deploy your policy now, or schedule it for later. Do one of these tasks:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Cancel a policy deployment

After you click **Deploy**, Catalyst Center begins to configure the policy on the devices in the site scope. If you realize that you made a mistake, you can cancel the policy deployment.

The policy configuration process is performed as a batch process, in that it configures 40 devices at a time. If you have 40 devices or fewer and you cancel a policy deployment, your devices might be configured anyway, because the deployment to the first batch of devices would have already taken place. However, if you have hundreds of devices, canceling the policy deployment can be useful when needed.

When you click **Abort**, Catalyst Center cancels the configuration process on devices whose configuration has not yet started, and changes the device status to **Policy Aborted**. Catalyst Center does not cancel the deployments that are in the process of being completed or have been completed. These devices retain the updated policy configuration and reflect the state of the policy configuration, whether it is Configuring, Successful, or Failed.

During a policy deployment, click **Abort** to cancel the policy configuration process.

Delete an application policy

You can delete an application policy if it is no longer needed.

When a policy is deleted, it removes the class maps, the policy map, and the association of the policy map with the wireless policy profile.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to delete.

Step 3 Click the radio button next to the policy that you want to delete.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Delete policy from devices** radio button and click **Apply**.

Step 6 To confirm the deletion, click **OK**. Otherwise, click **Cancel**.

Step 7 When the deletion confirmation message appears, click **OK** again.

You can view the deletion status of the policies in the **Application QoS Policies** window. If the status shows deletion failed, do these steps:

a) Click the failed state link under **Deployment Status** in the **Application QoS Policies** window.
b) In the **Undeployment Status** window, click **Retry** to delete the policy.

Clone an application policy

If an existing application policy has most of the settings that you want in a new policy, you can save time by cloning the existing policy, changing it, and then deploying it to a different scope.

Before you begin

You must have created at least one policy.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to clone.

Step 3 Click the radio button next to the policy that you want to clone.

Step 4 From the **Actions** drop-down list, choose **Clone**.

Step 5 Configure the application policy, as needed. For information about the application policy settings, see Create an application policy, on page 1231.

Step 6 Do one of these tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy drafts, on page 1227.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Run Now** radio button and click **Apply**.

  To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see Policy scheduling, on page 1228.

Note The site time zone setting is not supported for scheduling application policy deployments.

Restore an application policy

If you create or make changes to a policy and then decide that you want to start over, you can restore the original QoS configuration that was on the device before you configured it using Catalyst Center.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to reset.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Restore devices to original configurations** radio button and click **Apply**.

Step 6 Click **OK** to confirm the change or **Cancel** to cancel it.

You can view the restoration status of the policies in the **Application QoS Policies** window. If the status shows restoration failed, do these steps:

a) Click the failed state link under **Deployment Status** in the **Application QoS Policies** window.

b) In the **Undeployment Status** window, click **Retry** to restore the policy.

Reset the default CVD application policy

The CVD configuration is the default configuration for applications. If you create or make changes to a policy and then decide that you want to start over, you can reset the applications to the CVD configuration. For more information about the CVD configuration, see Application policies overview, on page 1217.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to reset.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **Reset to Cisco Validated Design**.

Step 6 Click **OK** to confirm the change or **Cancel** to cancel it.

Step 7 Do one of these tasks:

- To save a draft of the policy, click **Save Draft**.
- To deploy the policy, click **Deploy**.

  Depending on Visibility and Control of Configurations settings, you can either:

  - Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
  - Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Display application policy history

You can display the version history of an application policy. The version history includes the series number (iteration) of the policy and the date and time on which the version was saved.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Click the radio button next to the policy that interests you.

Step 3 From the **Actions** drop-down list, choose **History**.

Step 4 From the **Policy History** dialog box, you can do these tasks:

- To compare a version with the current version, click **Difference** next to the version that interests you.

- To roll back to a previous version of the policy, click **Rollback** next to the version that you want to roll back to.

Roll back to a previous policy version

If you change a policy configuration, and then realize that it is incorrect, or that is not having the desired affect in your network, you can revert to a policy that is up to five versions back.

Before you begin

You must have created at least two versions of the policy to roll back to a previous policy version.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Click the radio button next to the policy that interests you.

Step 3 From the **Actions** drop-down list, choose **Show History**.

Previous versions of the selected policy are listed in descending order, with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.

Step 4 (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.

Step 5 When you determine the policy version that you want to roll back to, click **Rollback** for that policy version.

Note If the selected site scope changed between policy versions, rollback is not done on the current (latest) selected site. Only the policy content is rolled back.

Step 6 Click **Ok** to confirm the rollback procedure.

The rolled back version becomes the newest version.

Manage queuing profiles

These sections provide details about the various tasks that you can perform to manage queuing profiles.

Create a queuing profile

Catalyst Center provides a default CVD queuing profile (CVD_QUEUING_PROFILE). If this queuing profile does not meet your needs, you can create a custom queuing profile.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Queuing Profiles**.

Step 2 Click **Add Profile**.

Step 3 In the **Profile Name** field, enter a name for the profile.

Step 4 Configure the bandwidth for each traffic class by using the slider, clicking the plus (+) or minus (-) sign, or entering a specific number in the field.

The number indicates the percentage of the total interface bandwidth that will be dedicated to the selected application class. Because the total bandwidth equals 100, adding bandwidth to one application class subtracts bandwidth from another application class.

An open lock icon indicates that you can edit the bandwidth for the application class. A closed lock indicates that you cannot edit it.

If you make a mistake, you can return to the CVD settings by clicking **Reset to Cisco Validated Design**.

The graph in the middle helps you visualize the amount of bandwidth that you are setting for each application class.

Step 5 (For advanced users) To customize the DSCP code points that Catalyst Center uses for each of the traffic classes, from the **Show** drop-down list, choose **DSCP Values** and configure the value for each application class by entering a specific number in the field.

To customize the DSCP code points required within a service provider cloud, configure a service provider profile.

Step 6 Click **Save**.

Edit or delete a queuing profile

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Queuing Profiles**.

Step 2 From the **Queuing Profile** pane, click the radio button next to the queuing profile that you want to edit or delete.

Step 3 Do one of these tasks:

- To edit the profile, change the field values, except the profile name, and click **Save**. For information about the fields, see Create a queuing profile, on page 1241.
- To delete the profile, click **Delete**.

  You cannot delete a queuing profile if it is referenced in an application policy.

Manage application policies for WAN interfaces

These sections provide details about the various tasks that you can perform to manage application profiles for WAN interfaces.

Customize service provider profile SLA attributes

If you do not want to use the default SLA attributes assigned to your service provider profile by its class model, you can customize the service provider profile SLA attributes to fit your requirements. For more information about the default service provider profile SLA attributes, see Service provider profiles, on page 1222.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to change.

Step 3 Select the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **SP Profiles** and choose a service provider profile.

Step 6 You can modify the information in these fields:

- **DSCP**: Differentiated Services Code Point (DSCP) value. Valid values are from 0 to 63.
  - Expedited Forwarding (EF)
  - Class Selector (CS): CS1, CS2, CS3, CS4, CS5, CS6
  - Assured Forwarding: AF11, AF21, AF41
  - Default Forwarding (DF)

  For more information about these DSCP values, see Marking, queuing, and dropping treatments, on page 1219.
- **SP Bandwidth %**: Percentage of bandwidth allocated to a specific class of service.
- **Queuing Bandwidth %**: Percentage of bandwidth allocated to each of the traffic classes. You can make one of these changes:
  - To customize the queuing bandwidth, unlock the bandwidth settings by clicking the lock icon and adjust the bandwidth percentages.
  - To calculate the queuing bandwidth automatically from the service provider bandwidth, lock the queuing bandwidth settings by clicking the lock icon and then clicking **OK** to confirm. By default, Catalyst Center automatically distributes the queuing bandwidth percentage such that the sum of the queuing bandwidth for all of the traffic classes in a service provider class aligns with the service provider bandwidth percentage of that class.

Step 7 Click **OK**.

Assign a service provider profile to a WAN interface

If you have already created an application policy and now want to assign service provider profiles to WAN interfaces, you can edit the policy and perform this configuration, including setting the subline rate on the interface, if needed.

Before you begin

If you have not created a policy, you can create a policy and assign service provider profiles to WAN interfaces at the same time. For more information, see Create an application policy, on page 1231.

Procedure

Step 1 From the main menu, choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to edit.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 From the **Site Scope** pane, click the gear icon next to the site you are interested in.

Step 6 Click **Configure** in the **SP Profile Settings** column for the device you are interested in.

Step 7 In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.

Step 8 In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:

- **Physical interface**: Choose **WAN**. This role is the only valid role for a physical interface.
- **Tunnel interface**: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.



Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

Step 9 In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose a service provider profile.

Step 10 If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.

Step 11 To configure additional WAN interfaces, click **+** and repeat Step 7 through Step 10.

Step 12 Click **Save**.

Step 13 Click **< Back to Site Scope**.

Step 14 Click **OK**.

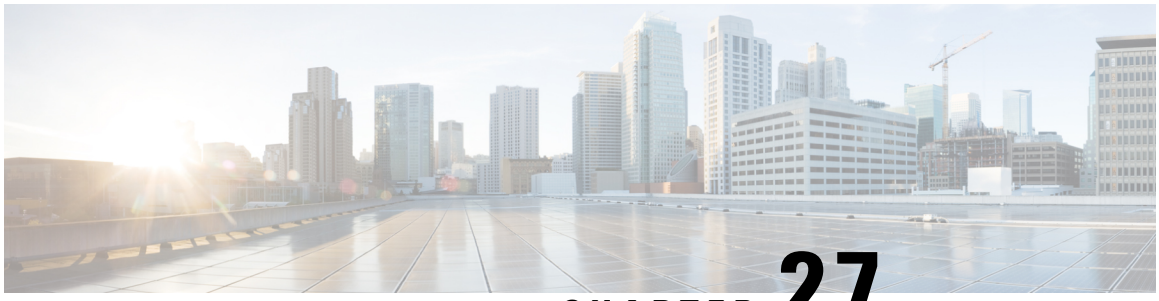
Step 15 Click **Deploy**.

You are prompted to deploy your policy now or to schedule it for a later time.

Step 16 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.



CHAPTER 27

Configure Traffic-Copy Policies

- Traffic copy policies, on page 1247
- Sources, destinations, and traffic copy destinations, on page 1247
- Guidelines and limitations of traffic copy policy, on page 1248
- Workflow to configure a traffic copy policy, on page 1249
- Create a traffic copy destination, on page 1249
- Edit or delete a traffic copy destination, on page 1250
- Create a traffic copy contract, on page 1250
- Edit or delete a traffic copy contract, on page 1250
- Create a traffic copy policy, on page 1251
- Edit or delete a traffic copy policy, on page 1251

Traffic copy policies

Using Catalyst Center, you can set up an Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration such that the IP traffic flow between two entities is copied to a specified destination for monitoring or troubleshooting.

To configure ERSPAN using Catalyst Center, create a traffic copy policy that defines the source and destination of the traffic flow that you want to copy. You can also define a traffic copy contract that specifies the device and interface where the copy of the traffic is sent.

Note Because traffic copy policies can contain either security groups or IP network groups, throughout this guide, we use the term *groups* for both security groups and IP network groups, unless specified otherwise.

Sources, destinations, and traffic copy destinations

Catalyst Center simplifies the process of monitoring traffic. You do not have to know the physical network topology. You only have to define a source and destination of the traffic flow and the traffic copy destination where you want the copied traffic to go.

- **Source**: One or more network device interfaces through which the traffic that you want to monitor flows. The interface might connect to endpoint devices, specific users of these devices, or applications. A source

group comprises Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or port channel interfaces only.

- **Destination**: The IP subnet through which the traffic that you want to monitor flows. The IP subnet might connect to servers, remote peers, or applications.
- **Traffic Copy Destination**: Layer 2 or Layer 3 LAN interface on a device that receives, processes, and analyzes the ERSPAN data. The device is typically a packet capture or network analysis tool that receives a copy of the traffic flow for analysis.



Note At the destination, we recommend that you use a network analyzer, such as a Switch Probe device, or other Remote Monitoring (RMON) probe, to perform traffic analysis.

The interface type can be Ethernet, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces only. When configured as a destination, the interface can be used to receive only the copied traffic. The interface can no longer receive any other type of traffic and cannot forward any traffic except that required by the traffic copy feature. You can configure trunk interfaces as destinations. This configuration allows the interfaces to transmit encapsulated traffic.



Note There can be only one traffic copy destination per traffic copy contract.

Catalyst Center supports traffic copy policy on these devices:

- Source: Cisco Catalyst 3000, Catalyst 4000, Catalyst 9000
- Destination: Cisco Nexus 7000, ASR 1000, Catalyst 6000, ISR 4000

Guidelines and limitations of traffic copy policy

The traffic copy policy feature has these limitations:

- You can create up to 8 traffic copy policies, 16 copy contracts, and 16 copy destinations.
- The same interface cannot be used by more than one traffic copy destination.
- Catalyst Center does not show a status message to indicate that a traffic copy policy has been changed and is no longer consistent with the one that is deployed in the network. However, if you know that a traffic copy policy has changed since it was deployed, you can redeploy the policy.
- You cannot configure a management interface as a source group or traffic copy destination.

Workflow to configure a traffic copy policy

Before you begin

- To be monitored, a source security group that is used in a traffic copy policy needs to be statically mapped to the switches and their interfaces.

  For more information about creating a security group and assigning a security group to a source port, see Create a security group, on page 1186 and Configure ports within the fabric site, on page 1036.

- A traffic copy policy destination group needs to be configured as an IP network group. For more information, see Create an IP Network Group, on page 1212.

Procedure

Step 1 Create a traffic copy destination.

This is the interface on the device where the traffic flow will be copied for further analysis. For information, see Create a traffic copy destination, on page 1249.

Step 2 Create a traffic copy contract.

The contract defines the copy destination. For information, see Create a traffic copy contract, on page 1250.

Step 3 Create a traffic copy policy.

The policy defines the source and destination of the traffic flow and the traffic copy contract that specifies the destination where the copied traffic is sent. For information, see Create a traffic copy policy, on page 1251.

Create a traffic copy destination

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Copy** > **Traffic Copy** > **Traffic Copy Destination**.

Step 2 Enter a name and description for the traffic copy destination.

Step 3 Select the device and one or more ports.

Step 4 Click **Save**.

Edit or delete a traffic copy destination

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Copy** > **Traffic Copy Destination**.

Step 2 Check the check box next to the destination that you want to edit or delete.

Step 3 Do one of these tasks:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the destination, click **Delete**.

Create a traffic copy contract

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Copy** > **Traffic Copy Contract**.

Step 2 Click **Add**.

Step 3 In the dialog box, enter a name and description for the contract.

Step 4 From the **Copy Destination** drop-down list, choose a copy destination.

Note You can have only one destination per traffic copy contract.

If no copy destinations are available for you to choose, you can create one. For more information, see Create a traffic copy destination, on page 1249.

Step 5 Click **Save**.

Edit or delete a traffic copy contract

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Copy** > **Traffic Copy Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete.

Step 3 Do one of these steps:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the contract, click **Delete**.

Create a traffic copy policy

Procedure

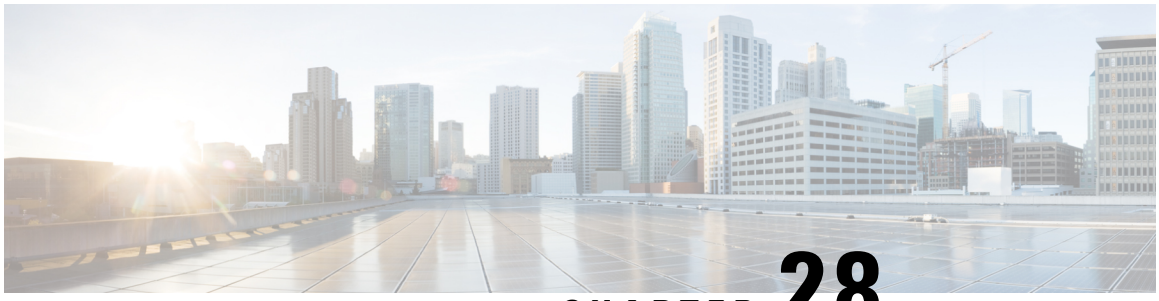
Step 1 From the main menu, choose **Policy** > **Traffic Copy** > **Traffic Copy Policies** .
Step 2 Click **Add Policy**.
Step 3 In the **Policy Name** field, enter a name.
Step 4 In the **Description** field, enter a word or a phrase that identifies the policy.
Step 5 In the **Contract** field, click **Add Contract**.
Step 6 Click the radio button next to the contract that you want to use and then click **Save**.
Step 7 Drag and drop groups from the **Available Groups** area to the **Source** area.
Step 8 Drag and drop groups from the **Available Groups** area to the **Destination** area.
Step 9 Click **Save**.

Edit or delete a traffic copy policy

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Copy** > **Traffic Copy Policies**.
Step 2 Check the check box next to the policy that you want to edit or delete.
Step 3 Do one of these tasks:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the policy, click **Delete**.



CHAPTER 28

Configure Rule-Based Compliance Policies

- Rule-based compliance policies, on page 1253
- Create a rule-based compliance policy, on page 1254
- Export a compliance policy as XML from Cisco Prime Infrastructure and import into Catalyst Center, on page 1263
- Export a rule-based compliance policy from Catalyst Center and import it into another Catalyst Center, on page 1264

Rule-based compliance policies

Rule-based compliance enables you to create custom configuration rules and policies that Catalyst Center periodically evaluates across your network to detect any violations. Platform-specific compliance policy rules can use string comparisons, regular expressions, and expression evaluations. These apply to configurations, CLI show commands, and device properties. Each rule can have variables, multiple conditions, and configurable violation messages, along with the severity level of the violation.

For example you can configure policies that:

- Ensure that ACL logging is off.
- Ensure that Telnet is disabled in the network.
- Ensure that the login authentication uses an external AAA server.
- Configure a minimum number of RADIUS servers.
- Configure the DHCP lease time for a specific number of days.
- Check that a console connection is allowed.
- Enable tracking of failed login attempts.
- Verify the password policy.

Scale Considerations

Rule-Based Compliance must provide flexibility in defining policies, rules, and conditions. However it should also have limits to prevent overload.

These limits are recommended at both the system and per-device levels.

Category	System Limit	Individual Limits
Policies	500	
Rules	5000	One policy: Up to 20 rules
Variables	12,500 (50% of rules use variables, avg. 5 per rule)	One rule: Up to 10 variables
Conditions	25,000 (avg., 5 conditions per rule	One rule: Up to 10 conditions

Create a rule-based compliance policy

Use this procedure to create a rule-based compliance policy.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 Click **Create Policy**.

a. In the **Create compliance policy** slide-in pane, enter the name of the policy in the **Policy Name** field.

b. In the **Description** field, enter an optional description.

c. Click **Save**.

Create rule-based compliance policy rules

Use this procedure to create a new rule for the rule-based compliance policies.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule-Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 (Optional) In the **Rule** pane, click **Add rule** to add a new rule and complete these configurations:

a) In the **Rule name** field, enter the name of the rule.

b) In the **Description** field, enter a description of the rule.

c) (Optional) Expand **Add impact and suggested fix** and configure these values:

- **Impact** - enter a brief note on the impact of the violation that the rule will generate
- **Suggested fix** - enter a brief note on the suggested fix for the violation that the rule will generate

Note The rule runs only on the devices that match the selected criteria. If you have selected only a device family or device series, the rule is applicable for all devices under the device family or device series.

Step 4 From the **Software type** drop-down list, select the software type as **IOX**, **IOS-XE**, or **Cisco Controllers**.

Step 5 From the **Device family** drop-down list, select the device family as **Routers**, **Switches and Hubs**, or **Wireless Controllers**.

Step 6 Click either the **Device series** or **Device models** toggle button.

Step 7 Select the check boxes for the device series or device models to which you want to apply the rule.

Step 8 Click **Save** to create the rule.

Add a condition to the compliance policy rule

Use this procedure to add a condition to the rule-based compliance policy rule.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule -Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 In the **Rules** pane, In the Rules pane, click the name of the rule.

Step 4 Expand the **Conditions** pane. Click **Add Condition**.

Step 5 In the **Add Conditions** pane, add a condition to the rule.

a) Configure the condition based on if you want to configure basic or advance settings.

b) If you want to configure a basic settings, expand the **Conditions** pane.

c) From the **Scope** drop-down list, select the scope of the condition and complete these configurations for the basic settings.

Table 71: Basic settings

If you chose..	Then...
Configuration	From the **Operator** drop-down list, select the operator required for the selected scope. • Contains the string • Does not contain the string • Matches the expression • Does not match the expression • Evaluate expression Enter the value in the **Value** field. Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.
Device command outputs	In the **Show command** field, select the show command or enter the custom show command to add it to the list. From the **Operator** drop-down list, select the operator required for the selected scope. • Contains the string • Does not contain the string • Matches the expression • Does not match the expression • Evaluate expression Enter the value in the **Value** field. Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

Expand **Actions** pane and complete these configurations for basic settings:

If you chose...	Then...
Continue	proceed without raising a violation.

If you chose...	Then...
Raise a violation and continue	configure the severity of the violation based on the scope of the condition. • From the **Violation severity** drop-down list, choose the severity of the violation. • In the **Custom violation message** field, enter an optional user- defined violation message. • Configure Fix CLI for Remediation: In the **Fix CLI** section, select the **Template language** as **JINJA** or **VELOCITY**. • In text editor, enter the CLI command in remediate the violation.

d) If you want to configure a advance condition, enable **Advance settings** in the **Add condition** pane, to access additional options for parsing the configurations and performing actions.

e) Expand the **Conditions** pane. From the **Scope** drop-down list, select the scope of the condition and complete these configurations for the advanced settings.

Table 72: Advanced settings

If you chose..	Then...

Configuration	check the **Parse as Blocks** check box to split entire running configurations into blocks and search for the condition match criteria value within each block.
	
	Enter the **Block start expression** and **Block end expression**. The blocks are split based on the start and end expressions.
	
	(Optional) Click **Advance block options** to choose the violation options.
	
	• **Raise violation if ANY block has a violation**: Single or multiple violations can be raised.
	  • **Raise multiple violations - one violation per violating block**: Execution continues for all blocks and raises as many violations.
	  • **Raise a single violation for all violating blocks**: Execution stops if system finds one block with a violation.
	
	• **Raise violation only if ALL blocks have a violation**: Only one violation is raised for the rule.
	
	From the **Operator** drop-down list, select the operator required for the selected scope.
	
	• Contains the string
	• Does not contain the string
	• Matches the expression
	• Does not match the expression
	• Evaluate expression
	
	In the **Value** field, enter the value.
	
	Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

If you chose..	Then...
Device command outputs	In the **Show command** field, select the show command or enter the custom show command to add it to the list. From the **Operator** drop-down list, select the operator required for the selected scope. • Contains the string • Does not contain the string • Matches the expression • Does not match the expression • Evaluate expression In the **Value** field, enter the value. Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

Expand **Actions** pane and complete these configurations:

If you chose...	Then...
Match Action as **Continue**	proceed to check the next condition, if present, without raising a violation.
Select Does Not Match Action as **Raise a violation and continue**	raises violation by configuring the severity of the violation and violation message. • From the **Violation severity** drop-down list, choose the severity of the violation. • In the **Custom violation message** field, enter an optional user- defined violation message.

Example: Block Options

This compliance policy checks if there are any rogue or unauthorized SNMP community strings are defined in the given blocks. If they are detected in the blocks, the policy raises a violation with the message “Detected unauthorized community string <1.1>” and removes all non-compliant SNMP strings from the blocks.

Pane	Pane Area	Field	Value
Rule Information		Rule Title	snmp-server community having non-standard entries

Pane	Pane Area	Field	Value
Platform Selection			Cisco IOS Devices, Cisco IOS-XE Devices
Condition 1			
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community (.*)
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Does Not Raise a Violation
Condition 2			
Condition Details	**Condition Scope Details**	Condition Scope	Previously Matched Blocks
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks check box is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community ((public RO)|(private RW))
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Detected unauthorized community string <1.1>.

Note In the above example, the matching criteria will be termed as 1.1, 1.2, and so on, for first condition. For the second condition, the matching criteria will be termed as 2.1, 2.2, and so on.

Example Conditions and Actions: NTP Server Redundancy

This compliance policy checks if the command **ntp server** appears at least twice on the device. If it does not, the policy raises a violation with the message "At least two NTP servers must be configured."

Pane	Pane Area	Field	Value
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	(ntp server.*\n){2,}
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	At least two NTP servers must be configured.

Add a variable to the policy rule

Use this procedure to add a new variable to the rule-based compliance policy rule.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule-Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 In the **Rules** pane, click the name of the rule.

Step 4 (Optional) Expand the **Variables** pane. Click **Add Variable** to add a variable to the rule.

a) Enter the variable name, identifier, and description in the corresponding fields.

b) Expand the **Data type** pane and choose the data type.

If you chose...	Then...
String	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Is list of values** check box to provide the list of values for the rule variable. **3.** Click **Add**; then add the name and value in the corresponding fields. Click **Save**. **4.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value. Use integer for integer data type. **Maximum length**: Enter the maximum length of the string. **Valid regex**: Enter a valid regular expression to validate the string input.
Integer	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Is list of values** check box to provide the list of values for the rule variable. **3.** Click **Add**; then add the name and value in the corresponding fields. Click **Save**. **4.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value. Use integer for integer data type. **Minimum value**: Enter the minimum value for an integer. **Maximum value**: Enter the maximum value for an integer.
Boolean	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Is list of values** check box to provide the list of values for the rule variable. **3.** Click **Add**; then add the name and value in the corresponding fields. Click **Save**. (optional) **Default value**: Choose **true** or **false**.
IP address	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value.
Interface	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value.

If you chose...	Then...
IP mask	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check to specify the values for the rule variable. (optional) **Default value**: Enter the default value.

c) The **Preview** section displays the preview of the configured variable. Click **Save**.

Assign a policy to sites

Use this procedure to assign a rule-based compliance policy to sites.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule-Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 In the **Sites** pane, click **Assign to sites** in the top-right corner.

Alternatively, to assign from the policy table, check the corresponding check box and in the **Sites** column, click **Assign**.

Step 4 In the **Assign to sites** slide-in pane, check the check box next to the sites to in the site hierarchy to select them and click **Assign**.

The policy applies to eligible devices at the selected sites.

Export a compliance policy as XML from Cisco Prime Infrastructure and import into Catalyst Center

Use this procedure to export compliance policies from Cisco Prime Infrastructure as XML and import into Catalyst Center.

- You can export and import individual compliance policies into another server, if needed.

Procedure

Step 1 From the Cisco Prime Infrastructure GUI, choose **Configuration > Compliance > Policies**.

Step 2 Export a compliance policy:

a) From the **Compliance Policies** navigation area, hover your cursor over the **i** icon next to the policy.

b) In the pop-up window, click the **Export Policy as XML** hyperlink, and save the file.

Step 3 Import a compliance policy to Catalyst Center:

a) From the top-left corner, click the menu icon and choose **Policy** > **Rule-Based Compliance Policies**.
b) Click **Import policies** to open the **Import compliance policy** slide-in pane.
c) In the **Import compliance policy** slide-in pane, drag and drop your XML file into the upload area. Alternatively, click on **Click or drag files to this area to upload**, locate your XML file, and then click **Import**.

Export a rule-based compliance policy from Catalyst Center and import it into another Catalyst Center

Use this procedure to export compliance policies from Catalyst Center and import into another Catalyst Center instance.

- You can import JSON files primarily used for exporting policies between Catalyst Center instances.
- You can import individual compliance policies and, if needed, transfer them to another server.
- The activity center page offers details on both successful and failed imports, making it easier to monitor and troubleshoot policies.

Procedure

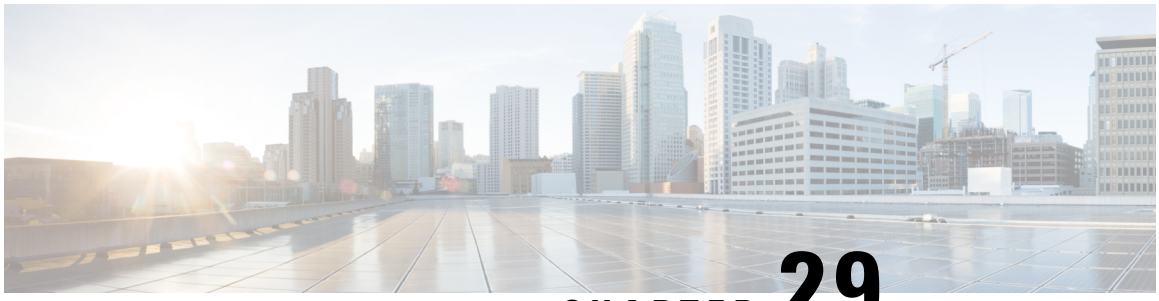
Step 1 From the top-left corner, click the menu icon and choose **Policy > Rule-Based Compliance Policies**.

Step 2 Export a compliance policy:

a) In the policy table, check the check box next to the desired policy..
b) Click **Export**. Extract the JSON file from the ZIP file and save it to your local desktop.

Step 3 Import a compliance policy to Catalyst Center:

a) Click **Import policies** to open the **Import compliance policy** slide-in pane.
b) In the **Import compliance policy** slide-in pane, Drag and drop your XML file into the upload area. Alternatively, click on **Click or drag files to this area to upload**, locate your XML file, and then click **Import**.



CHAPTER 29

Configure Traffic Steering Policies

- Traffic steering policy overview, on page 1265
- Traffic steering policies, on page 1266
- Traffic steering contracts, on page 1270

Traffic steering policy overview

Traffic steering policies determine which traffic is sent to the firewall in a network for security service insertion (SSI).

These policies contain

- security groups (source and destination security groups),
- firewall, and
- traffic steering contracts.

Overview window

The traffic steering policy **Overview** window provides a summary of the security service insertion configuration.

From the main menu, choose **Policy** > **Traffic Steering Policy** to view the **Overview** window.

This table provides information about the components of this window based on the status of security service insertion.

If security service insertion is...	Then...
disabled	this window displays the **Enable Service Insertion** option to enable security service insertion. For more information, see Enable a service insertion site, on page 1164.

If security service insertion is...	Then...

enabled	this window displays these areas:
	• **Summary**: displays the total number of:
	  • Service insertion sites
	  • Policies
	  • Traffic steering contracts
	• **Statistics by configuration**: displays this information:
	  • Top five firewall IP addresses
	  • Top five traffic steering contracts
	  • Top five nodes

Traffic steering policies

For a service insertion site, the **Traffic steering policies** tab displays the steering policy details in the matrix view and list view.

Matrix view

Click the icon on the top-right corner to open the matrix view. Matrix view provides an overview of all policies for all the security groups.

The matrix view contains two axes:

- Source axis: the vertical axis lists all the source security groups.
- Destination axis: the horizontal axis lists all the destination security groups.

Each cell in the matrix displays a color based on the type of policy configured for the corresponding source and destination security group:

- traffic steering policy,
- group-based policy,
- both traffic steering and group-based policies,
- no policy, or
- policies not applicable

Click to view the legend.

For the source and destination security group pairs that have a traffic steering policy configured, you can click the corresponding cell to view the traffic steering policy details and edit it. For source and destination security group pairs that do not have a traffic steering policy configured, you can click the corresponding cell to create the policy.

You can also create and deploy the traffic steering policies in this view.

List view

Click the icon on the top-right corner to open the list view. List view provides a list of all the available traffic steering policies.

In this view, you can create, edit, view, delete, and deploy the traffic steering policies.

Create a traffic steering policy on day zero

Use this procedure to create a traffic steering policy on day zero.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering policies** tab.

Step 3 Click **Enable Service Insertion** to enable service insertion and create a traffic steering policy during the workflow.

For information about enabling service insertion, see Enable a service insertion site, on page 1164.

Create a traffic steering policy on day *n*

Use this procedure to create a traffic steering policy on day *n*.

When you create a traffic steering policy, Catalyst Center creates a corresponding mirror policy automatically to reverse the traffic.

Before you begin

- Ensure that the prerequisites are met. For more information, see Prechecks to enable a service insertion site on day zero, on page 1162.
- Enable security service insertion in Catalyst Center. For more information, see Enable a service insertion site, on page 1164.

Note If the security service insertion is not enabled, then Catalyst Center does not allow you to create the traffic steering policy.

- Create a traffic steering contract. For more information, see Create a traffic steering contract, on page 1270.
- Create a Layer 3 virtual network. For more information, see Create a Layer 3 virtual network, on page 1040.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering policies** tab.

Step 3 From the **Fabric site** drop-down list, choose a fabric site.

Step 4 Click **Create policy**.

Step 5 From the drop-down lists, choose

- a source security group,
- destination security groups, and
- a traffic steering contract.

Note The source and destination security groups must be different.

Step 6 From the **Select a VN** drop-down list, choose a virtual network.

When you choose a virtual network, Catalyst Center displays the corresponding firewall name.

Step 7 (Optional) Click the + icon to add another virtual network and firewall.

Step 8 Under **Schedule provisioning**, choose a schedule.

a) In the **Task name** field, enter a name for the provisioning task.

b) Under **Schedule provisioning**, choose a schedule to push the policy to Cisco ISE.

Click...	To...
Now	Immediately deploy the configuration.
Later	Schedule the date and time and define the time zone of the deployment.

Step 9 Click **Save**.

What to do next

Deploy the policy on the device. For more information, see Deploy traffic steering policies, on page 1270.

Edit a traffic steering policy

Use this procedure to edit a traffic steering policy.

When you edit a traffic steering policy, Catalyst Center updates the corresponding mirror policy automatically. Catalyst Center uses the mirror policy to reverse the traffic.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering policies** tab.

Step 3 From the **Fabric site** drop-down list, choose a fabric site.

Step 4 In the list view ( ), check the check box next to the traffic steering policy that you want to edit.

Step 5 Hover your cursor over **Actions** and choose **Edit**.

Step 6 In the **Edit policy** slide-in pane, edit the required configurations.

For more information, see Create a traffic steering policy on day n, on page 1267.

Step 7 Under **Schedule provisioning**, choose a schedule.

a) In the **Task name** field, enter a name for the provisioning task.

b) Under **Schedule provisioning**, choose a schedule to push the policy to Cisco ISE.

Click...	To...
Now	Immediately deploy the configuration.
Later	Schedule the date and time and define the time zone of the deployment.

Step 8 Click **Save**.

What to do next

Deploy the policy on the device. For more information, see Deploy traffic steering policies, on page 1270.

Delete traffic steering policies

Use this procedure to delete traffic steering policies.

When you delete a traffic steering policy, Catalyst Center deletes the corresponding mirror policy automatically.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering policies** tab.

Step 3 From the **Fabric site** drop-down list, choose a fabric site.

Step 4 In the list view ( ), check the check box next to the traffic steering policies that you want to delete.

Step 5 Hover your cursor over **Actions** and choose **Delete**.

Step 6 In the warning dialog box, click **Delete**.

What to do next

Deploy the updates on the device. For more information, see Deploy traffic steering policies, on page 1270.

Deploy traffic steering policies

Use this procedure to deploy traffic steering policies to devices associated with the service insertion site after you create, edit, or delete traffic steering policies.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering policies** tab.

Step 3 From the **Fabric site** drop-down list, choose a fabric site.

Step 4 Click **Deploy**.

Step 5 In the **Schedule deployment** slide-in pane, schedule the deployment.

a) In the **Task name** field, enter a name for the task.

b) Choose the required option to schedule the deployment.

Option	Description
Now	Immediately deploy the configurations.
Later	Schedule the date and time, and define the time zone to deploy the configurations.

c) Click **Deploy**.

Traffic steering contracts

A traffic steering contract defines a set of rules that redirect specific network traffic from a source security group to destination security groups when the traffic matches a

- network application,
- transport protocol, and
- source and destination port.

Create a traffic steering contract

Use this procedure to create a traffic steering contract to redirect the traffic.

Catalyst Center creates the contracts at a global level and doesn't assign them to any site.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering contracts** tab.

Step 3 Click **Create steering contract**.

Step 4 In the **Steering contract name** field of the **Create a steering contract** slide-in pane, enter a name for the steering contract.

Step 5 (Optional) In the **Description** field, enter a description.

Step 6 Click **Add Rule** to add a rule and complete these configurations:

a) Under **Application**, choose the application for which you want to apply the rule.

1. Click the pencil icon.
2. In the **Choose Application** dialog box, choose the required application.
3. Click **Confirm**.

If you chose...	Then...
advanced	• Under **Transport Protocol**, from the drop-down list, choose a transport protocol for the rule. • Under **Source port** and **Destination port**, enter the corresponding port numbers for the rule. The valid range is from 1 to 65535.
other applications	based on the application that you chose, Catalyst Center displays the corresponding ports and transport protocol automatically.

b) Use the **Enable logs** toggle button to enable or disable logging for any traffic filter rule (including the default action).

By default, logging is disabled. When logging is enabled, the device sends a syslog message when the rule is triggered.

Logging can be helpful in troubleshooting and initial testing of a policy. However, we recommend that you use it sparingly, as it may impact the resources and performance of devices.

Step 7 (Optional) Complete these configurations:

If you want to...	Then...
create another rule	Use one of these options: • Repeat Step 6, on page 1271, or • under **Actions**, click the corresponding + icon and repeat 6.a, on page 1271 and 6.b, on page 1271.

If you want to...	Then...
Update the sequence of a rule.	The rules are checked in the sequence in which they are listed in the **Rules** table. Complete these steps to update the sequence: **a.** Click the corresponding icon. **b.** Drag and drop the rule to the required position.
Enable logs for multiple rules.	**a.** Check the check box next to the required rules. **b.** Click **Enable Logs**.
delete rules	**a.** Check the check box next to the rules that you want to delete and click **Delete**, or **b.** under **Actions**, click the corresponding delete icon () for the rule that you want to delete.

Step 8 Click **Save**.

Catalyst Center detects any duplicate rules and merges them automatically while saving the traffic steering contract.

Edit or duplicate a traffic steering contract

Use this procedure to edit or duplicate a traffic steering contract.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering contracts** tab.

Step 3 Check the check box next to the contract that you want to edit or duplicate.

Step 4 Choose the required option.

If you want to...	Then...
edit the steering contract	hover your cursor over **More Actions** and choose **Edit**.
duplicate the steering contract	hover your cursor over **More Actions** and choose **Duplicate**.

Step 5 Edit the required configurations.

For more information, see Create a traffic steering contract, on page 1270.

Step 6 Click **Save**.

Delete traffic steering contracts

Use this procedure to delete traffic steering contracts.

Procedure

Step 1 From the main menu, choose **Policy** > **Traffic Steering Policy**

Step 2 Click the **Traffic steering contracts** tab.

Step 3 Check the check box next to the contracts that you want to delete.

Step 4 Hover your cursor over **More Actions** and choose **Delete**.

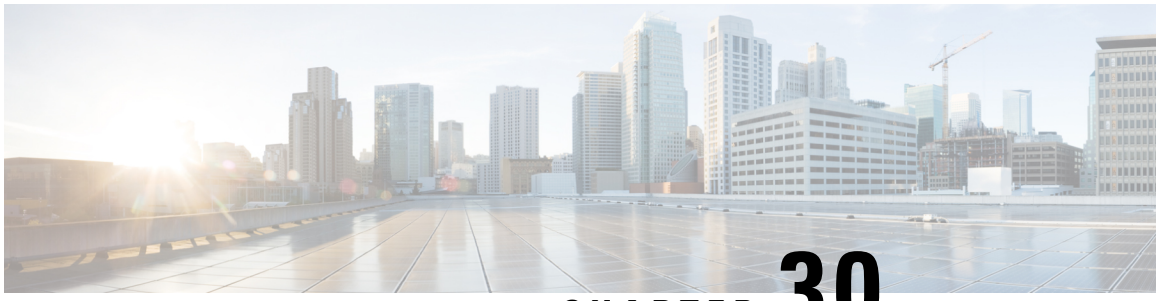
Step 5 In the warning dialog box, click **Yes**.



PART VII

Monitor and Troubleshoot Your Network

- Enable Advanced Feature Trials, on page 1277
- Cisco AI Endpoint Analytics, on page 1281
- Troubleshoot Network Devices Using Network Reasoner, on page 1331
- Identify Network Bugs, on page 1345
- Identify Network Security Advisories, on page 1349
- Identify Network Field Notices, on page 1367
- Generate the Root Cause Analysis File from Catalyst Center, on page 1369



CHAPTER 30

Enable Advanced Feature Trials

- Advanced Features trial overview, on page 1277
- Enable the Network Bug Identifier trial, on page 1277
- Enable the Security Advisories trial, on page 1278
- Enable the Field Notices trial, on page 1278

Advanced Features trial overview

Advanced Features trials are free for a limited time. These features work with the CX Cloud to provide customized insights based on your operational data and network configuration. By authorizing the CX Cloud Consent to Connect agreement through the Catalyst Center dashboard, you can enable access to the advanced features.

These advanced features help secure and keep your network up to date. Using advanced machine learning algorithms, Cisco scans and analyzes your hardware, software, and device configuration to generate customized and actionable insights specific to your environment.

Note

- When you enable these advanced features, Catalyst Center sends data to the U.S.-hosted CX Cloud only, not to other regions.
- The EoX (End of Life milestones) feature is offered independent of the Advanced Features trial. To enable access to the EoX feature, authorize the CX Cloud Consent to Connect agreement through the Catalyst Center dashboard. For information about the EoX feature, see Compliance categories, on page 562.

Enable the Network Bug Identifier trial

You can try out this feature by enabling the CX license for a 90-day trial.

Before you begin

- You must enter the correct URL and port in your firewall for Catalyst Center to reach the CX Cloud.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Bug Identifier**.

If the feature trial hasn't started yet, Catalyst Center displays a banner with the trial offer. If the feature trial has started already, the number of days left in the trial displays.

Step 2 To begin the trial, you must accept the trial terms and conditions:

- If you've already accepted the trial terms and conditions for another feature trial or feature, continue to the next step.
- If you haven't accepted them yet, you are prompted to do so. In the banner, click the **Consent to Connect** link to display the trial terms and conditions and confirm that you've read and agree to them.

Step 3 Confirm that you want to enable the trial.

Enable the Security Advisories trial

You can try out this feature by enabling the CX license for a 90-day trial.

Before you begin

- You must enter the correct URL and port in your firewall for Catalyst Center to reach the CX Cloud.

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

If the feature trial hasn't started yet, Catalyst Center displays a banner with the trial offer. If the feature trial has started already, the number of days left in the trial displays.

Step 2 To begin the trial, you must accept the trial terms and conditions:

- If you've already accepted the trial terms and conditions for another feature trial or feature, continue to the next step.
- If you haven't accepted them yet, you are prompted to do so. In the banner, click the **Consent to Connect** link to display the trial terms and conditions and confirm that you've read and agree to them.

Step 3 Confirm that you want to enable the trial.

Enable the Field Notices trial

You can try out this feature by enabling the CX license for a 90-day trial.

Before you begin

- You must enter the correct URL and port in your firewall for Catalyst Center to reach the CX Cloud.

Procedure

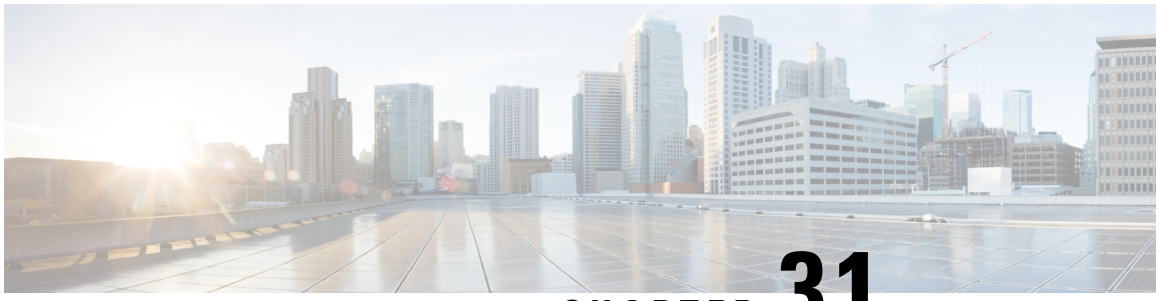
Step 1 From the main menu, choose **Tools** > **Field Notices**.

If the feature trial hasn't started yet, Catalyst Center displays a banner with the trial offer. If the feature trial has started already, the number of days left in the trial displays.

Step 2 To begin the trial, you must accept the trial terms and conditions:

- If you've already accepted the trial terms and conditions for another feature trial or feature, continue to the next step.
- If you haven't accepted them yet, you are prompted to do so. In the banner, click the **Consent to Connect** link to display the trial terms and conditions and confirm that you've read and agree to them.

Step 3 Confirm that you want to enable the trial.



CHAPTER 31

Cisco AI Endpoint Analytics

- Cisco AI Endpoint Analytics overview, on page 1281
- Key features of Cisco AI Endpoint Analytics, on page 1282
- FIPS compliance, on page 1283
- Set up Cisco AI Endpoint Analytics in Catalyst Center, on page 1283
- Cisco AI Endpoint Analytics overview window, on page 1287
- Endpoint Inventory, on page 1297
- Trust Score, on page 1302
- Profiling rules, on page 1318
- Cisco AI rules for smart grouping, on page 1324
- Hierarchy, on page 1327

Cisco AI Endpoint Analytics overview

Visibility is the first step towards securing an endpoint. Cisco AI Endpoint Analytics is an endpoint visibility solution that helps you identify and profile endpoints and Internet of Things (IoT) devices. The Cisco AI Endpoint Analytics engine enables you to assign labels to endpoints, using the telemetry information received from the network from various sources.

The profiling labels that are available in Cisco AI Endpoint Analytics are endpoint type, hardware model, manufacturer, and operating system type. This is called multifactor classification.

Cisco AI Endpoint Analytics provides nuanced visibility and enforcement in your network with features like Trust Scores that allow you to identify and act upon potentially risky endpoints and devices. You can also manage potential risks by applying ANC policies through Cisco ISE, from the Cisco AI Endpoint Analytics GUI. You can monitor and work around the issue of random and changing MAC addresses from endpoints in Cisco AI Endpoint Analytics and accurately identify endpoints through a unique attribute called the DUID instead of MAC addresses.

Cisco AI Endpoint Analytics helps you gather endpoint telemetry from different sources. The primary source is the Network-Based Application Recognition (NBAR) mechanism. The NBAR mechanism is embedded in Cisco Catalyst 9000 Series switches (access devices) and performs deep packet inspection (DPI). Cisco AI Endpoint Analytics can also receive telemetry from Catalyst Center Traffic Telemetry Appliance.

You can gather endpoint context information from various sources such as Cisco ISE, self-registration portals, and configuration management database (CMDB) software such as ServiceNow.

Cisco AI Endpoint Analytics allows data inflow from a wide range of network devices, expanding your ability to easily identify and profile endpoints with greater accuracy, and act upon any anomalies. You can aggregate

varied endpoint information and use the data to profile endpoints in Cisco AI Endpoint Analytics. After endpoints are profiled, AI and machine learning algorithms can also be used to reduce the number of unknown endpoints by intuitively leveraging different methods.

Key features of Cisco AI Endpoint Analytics

- **Cisco AI Endpoint Analytics dashboard**

  The Cisco AI Endpoint Analytics dashboard gives you a comprehensive view of the endpoints that are connected to your network. You can view the number of known, unknown, profiled, and unprofiled endpoints, endpoints with low Trust Scores, and endpoints that use random MAC addresses. The AI Proposals dashlet displays intelligent profiling suggestions to enhance endpoint profiling and management.

- **Trust Scores to flag potentially risky endpoints**

  Cisco AI Endpoint Analytics assigns Trust Scores to endpoints to allow you to easily monitor and act on potentially risky endpoints in your network. Behavioral anomalies are monitored and tracked, and a Trust Score is assigned based on the number and frequency of the anomalies tracked. See Trust Scores for endpoints, on page 1303.

- **Detect endpoints that use random MAC addresses**

  Cisco AI Endpoint Analytics enables you to handle the issue of random and changing MAC addresses by receiving from Cisco ISE a unique endpoint identifier called the DUID (also known as GUID in Cisco ISE). Cisco AI Endpoint Analytics then uses the DUID as the identifier for an endpoint, instead of its MAC address.

- **Reduce net unknowns with machine learning capabilities**

  Cisco AI Endpoint Analytics provides profiling suggestions based on learnings from endpoint groupings. You can use these suggestions to reduce the number of unknown or unprofiled endpoints in your network.

- **Manage endpoints with system and custom profiling rules**

  Use Cisco-provided system rules and custom rules of your design to reliably profile and manage the endpoints connected to your network.

- **Registration of endpoints through Cisco AI Endpoint Analytics**

  You can onboard and profile endpoints using Cisco AI Endpoint Analytics. The endpoint attribute data that is collected through this registration process is used to profile the endpoints.

- **Registration of endpoints using external sources**

  You can connect some external sources of endpoint data, such as Configuration Management Databases (CMDB), to Cisco AI Endpoint Analytics. This allows you to easily register, manage, and profile endpoints in your network.

- **Purge endpoints after a defined period of inactivity**

  Define an Endpoint Purge Policy to remove from your network the endpoints that have been inactive for a defined time. You can define the period of inactivity after which an endpoint must be removed. You can also customize a purge policy to act on a particular set of endpoints based on a profiling attribute.

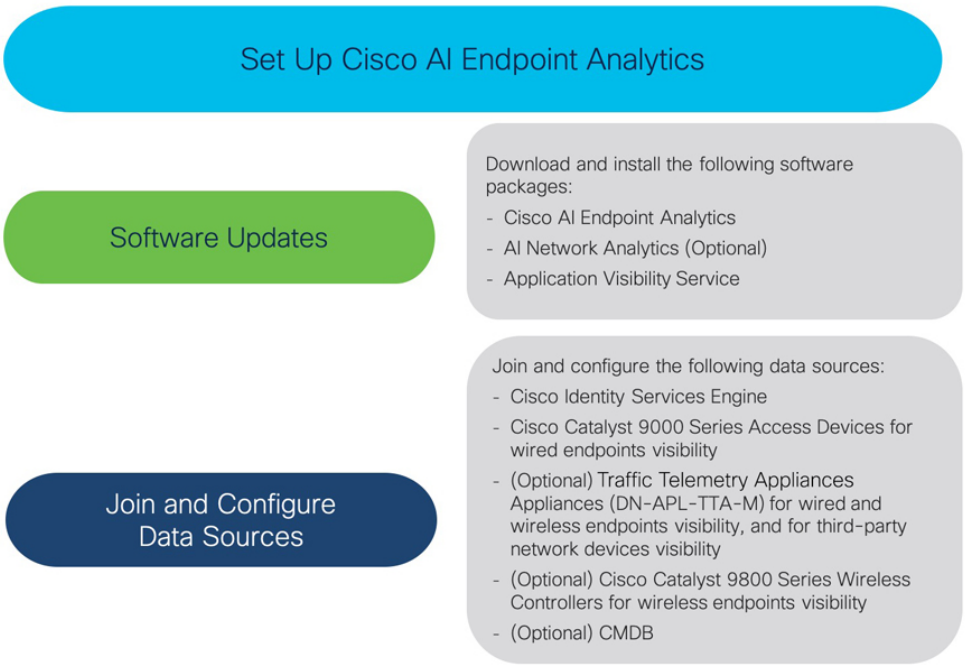
FIPS compliance

Catalyst Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Catalyst Center image. By default, FIPS mode is disabled.

When FIPS mode is enabled in Catalyst Center, these functions in the Catalyst Center GUI are *unavailable*:

- The **Enable AI Network Analytics** dashlet in the **Optional Configurations** section in **AI Endpoint Analytics Setup**.
- The **AI Proposals** dashlet in **Policy** > **AI Endpoint Analytics** > **Overview**.
- The **Profile Rule Settings** tab in **Policy** > **AI Endpoint Analytics** > **Overview** > **Configuration**.
- The **AI Spoofing Detection** section in **Policy** > **AI Endpoint Analytics** > **Overview** > **Configuration** > **Trust Analytics**.
- The **AI Spoofing Detection** section in **Endpoint Anomaly Detection** under **Trust Score** details for a particular endpoint in **Policy** > **AI Endpoint Analytics** > **Endpoint Inventory**.
- The **AI Spoofing Detection** column in **Policy** > **AI Endpoint Analytics** > **Endpoint inventory** > **Focus as Trust Score**.
- The **Talos IP Reputation** section in **Policy** > **AI Endpoint Analytics** > **Overview** > **Configuration** > **Trust Score Sources**.

Set up Cisco AI Endpoint Analytics in Catalyst Center



Install software updates

Install software updates in Catalyst Center to use Cisco AI Endpoint Analytics, as described in this procedure.

Procedure

Step 1 Log in to Catalyst Center.

Step 2 From the main menu, choose **System** > **Software Management**.

Step 3 In the **Updates** tab, check if **Cisco AI Endpoint Analytics**, **AI Network Analytics**, and **Application Visibility Service** are listed in the **Application Updates** section. If these application updates are visible, click **Install All**.

- Install the **Cisco AI Endpoint Analytics** update to access the endpoint profiling solution in your Catalyst Center.
- Install the **AI Network Analytics** update to use machine learning and AI capabilities to receive intelligent profiling suggestions.
- Install the **Application Visibility Service** update to use NBAR and Controller-Based Application Recognition (CBAR) techniques to inform endpoint profiling.

Step 4 If these updates aren't listed in the **Updates** tab, click the **Installed Apps** tab to check if the updates are already installed and are available for use. The **Currently Installed Applications** tab also confirms if the software installation succeeded.

Connect and enable data sources

The data sources that Cisco AI Endpoint Analytics uses may already be connected to your Catalyst Center. If the data sources are connected, follow these instructions to ensure that the data sources are available for use by Cisco AI Endpoint Analytics.

You must add Cisco ISE or Catalyst 9000 Series access devices to Catalyst Center for Cisco AI Endpoint Analytics to provide results.

Procedure

Step 1 Connect Cisco ISE to Catalyst Center:

See the "Integrate Cisco ISE with Catalyst Center" section in "Complete First-Time Setup" in the *Cisco Catalyst Center Installation Guide*.

These Cisco ISE releases support Cisco AI Endpoint Analytics:

- 2.4 Patch 11 and later
- 2.6 Patch 5 and later
- 2.7 Patch 1 and later
- 3.0 and later

For Cisco ISE 3.1 and later, in your Cisco ISE administration portal:

a) Choose **Work Centers** > **Profiler** > **Settings**.
b) In the **Endpoint Analytics Settings** area, check these check boxes:

- **Publish Endpoint Attributes to AI Endpoint Analytics**
- **Consume Endpoint Profiles from AI Endpoint Analytics**

After Cisco ISE authenticates endpoints through 802.1X or MAB authentication methods, the endpoint attributes collected are made available to Cisco AI Endpoint Analytics. Cisco ISE also shares telemetry data with Cisco AI Endpoint Analytics.

For Cisco ISE 2.4, 2.6, and 3.0, in your Cisco ISE administration portal:

a) Choose **Work Centers** > **Profiler** > **Settings**.
b) Choose the **Enable Probe Data Publisher** option.
c) Click **Save**.

Step 2 Connect Cisco 9000 Series access devices to Catalyst Center for wired endpoints visibility.

See "Discover Your Network" in the *Cisco Catalyst Center User Guide*.

To enable Cisco AI Endpoint Analytics features, upgrade your Cisco 9000 Series access devices to Cisco IOS-XE Release 17.6 or later.

To enable CBAR for the required access devices:

a) In the Catalyst Center GUI, click the menu icon and choose **Provision** > **Services** > **Application Visibility**.
b) Select the Cisco Catalyst 9000 access device that you need data from. Check the check box next to the device name in the **Site Devices** section.
c) Click **Enable CBAR**.
d) Click **Yes** in the subsequent confirmation window.
e) In the **Enable CBAR** slide-in pane, check the check box next to the supported SSID type.
f) Click **Enable**.

Step 3 (Optional) Connect Cisco Catalyst 9800 Series Wireless Controllers to Catalyst Center for wireless endpoints visibility.

These Cisco Catalyst 9800 Series Wireless Controller models are supported by Cisco AI Endpoint Analytics:

- 9800-CL
- 9800-40
- 9800-80
- 9800-L

Catalyst Center supports FlexConnect in Cisco Catalyst 9800 Series Wireless Controllers with Cisco IOS XE Release 17.7.1 and later.

To configure and provision a Cisco Catalyst 9800 Series Wireless Controller in Catalyst Center, see Cisco Catalyst 9800 Series Wireless Controller overview, on page 634.

Step 4 (Optional) Connect Cisco Catalyst IE9300 Rugged Series switches to Catalyst Center.

The Cisco Catalyst IE9300 Rugged Series switches are supported by Cisco AI Endpoint Analytics.

See “Discover Your Network” in the *Cisco Catalyst Center User Guide*.

Step 5 (Optional) Connect Catalyst Center Traffic Telemetry Appliance to Catalyst Center for wired and wireless endpoints visibility, and for third-party network device visibility.

Catalyst Center Traffic Telemetry Appliance (DN-APL-TTA-M) generates telemetry from mirrored network traffic for endpoint analytics. This appliance enables Network-Based Application Recognition-based (NBAR-based) protocol inspection and endpoint attribute extraction.

To receive endpoint attributes collected through the telemetry appliance in Cisco AI Endpoint Analytics, you must integrate Cisco ISE with Catalyst Center.

See Traffic Telemetry Appliances for information on installing the appliances, connectivity configurations, and managing the appliances in Catalyst Center.

Enable CBAR on Switched Port Analyzer (SPAN)-receiving ports of access switches connected to Catalyst Center Traffic Telemetry Appliance with this command:

```
ip nbar protocol-discovery
```

Not all endpoints that are connected to the telemetry appliances are visible in Cisco AI Endpoint Analytics. Only endpoints that are also connected to Network Access Devices (NADs) that are managed in Cisco Catalyst Assurance are visible in Cisco AI Endpoint Analytics.

Step 6 (Optional) Enable ServiceNow in Catalyst Center.

a) After connecting ServiceNow to Catalyst Center, click the menu icon and choose **Platform** > **Manage** > **Bundles**.
b) If the **Status** of the bundle **Endpoint Attribute Retrieval with ITSM (ServiceNow)** is **New**, click **Enable** for the bundle.

Step 7 (Optional) Enable Cisco AI Analytics in Catalyst Center.

To receive suggestions about AI-based endpoint groupings, automated custom profiling rules, and endpoint labels, and to detect potentially spoofed devices in your network, you must enable the required settings in the **Cisco AI Analytics** window.

You must install the AI Network Analytics software to receive these AI-based suggestions.

a) From the main menu, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**.
b) Click the toggle button for each of these services that you want to enable:

- **AI Endpoint Analytics**: AI Network Analytics leverages machine learning to drive intelligence in the network and enables you to effectively improve network performance and accelerate issue resolution. AI Network Analytics significantly reduces noise and false positives by analyzing network behavior and adapting to your network environment.
- **Endpoint Smart Grouping**: Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in your network by providing AI-based endpoint groupings, automated custom profiling rules, and crowdsourced endpoint labels.
- **AI Spoofing Detection**: AI Spoofing Detection identifies spoofed endpoints based on pretrained behavioral models. Enabling the **Enable AI Spoofing Detection** toggle button allows Catalyst Center to detect spoofed endpoints using these behavioral models and the flow information provided by the network devices. Several behavioral models are built and centrally trained using the collected flow information gathered from participating customers.
  - Spoofing detection is done in the cloud and anonymized data export to the cloud from Catalyst Center is mandatory. Catalyst Center then polls the cloud for spoofing detections.
  - An uninterrupted internet connection is required.

- While upgrading to the latest release, if data export was disabled in the previous release, a warning stating that data export is disabled is displayed upon upgrade. You must re-enable spoofing detection.

Endpoint telemetry sources

Cisco AI Endpoint Analytics receives telemetry data in these ways:

- **Deep packet inspection**

  Deep packet inspection is an advanced method of packet analysis that is carried out by Cisco Catalyst 9000 Series access devices. These access devices run NBAR, which inspects application traffic and performs protocol analysis to discover, identify, and profile endpoints with high fidelity.

  Deep packet inspection profiling is based on various attributes that are collected from endpoint traffic to the network. These attributes are collected across multiple protocols, from packet header layers 4 to 7.

- **Configuration Management Database Connection**

  Cisco AI Endpoint Analytics receives endpoint data from your Configuration Management Database Connection (CMDB) for greater accuracy in endpoint profiling. The connection with ServiceNow enables you to receive information from the CMDB to Cisco AI Endpoint Analytics.

- **Machine learning capabilities**

  Data collected for profiling is anonymized and sent to a Cisco cloud location that serves as a device data lake. Here, machine learning algorithms analyze the data available to create profiling rules that you can evaluate and apply, as needed. Smart profiling rules are suggested through Cisco AI Endpoint Analytics to help make endpoint profiling and management simpler and more efficient for you. Existing rules too are evaluated and improvement suggestions provided based on this continuous learning.

Cisco AI Endpoint Analytics overview window

From the main menu, choose **Policy** > **AI Endpoint Analytics**.

The **Overview** window displays these dashlets:

- **Total Endpoints**

  This dashlet displays the total number of endpoints in your network in two groups, **Fully Profiled** and **Partially Profiled**. Cisco AI Endpoint Analytics profiles endpoints based on four factors:

  - Endpoint type
  - OS type
  - Hardware model
  - Hardware manufacturer

  If one or more of these factors are missing for an endpoint, it is profiled in the **Partially Profiled** group.

Click **Partially Profiled Labels** to view the number of endpoints in your network with missing profiles, categorized by profile label type. To check the endpoints with a specific missing profile label, click the number next to the profile label. The **Endpoint Inventory** tab displays with the corresponding list of endpoints.

- **AI Proposals**

  Cisco AI Endpoint Analytics uses smart grouping algorithms to group unknown endpoints in your network that have similar profiling data. If you have enabled AI Endpoint Analytics, you will receive these types of rule proposals. These rule proposals are based on learnings from endpoint clusters:

  - New rules for profiling endpoints that may be similar.
  - Modification proposals for previously accepted rules.
  - Review of profiling rules that are no longer needed.

  For more details, see Cisco AI rules for smart grouping, on page 1324.

- **Trust Scores**

  The Trust Scores dashlet provides an overall view of the Trust Scores assigned to the endpoints in your network. See Trust Scores for endpoints, on page 1303.

- **Configuration**

  Click the **Configuration** link in the top-right corner of the **Overview** area to access these configurations:

  - **Profile Rule Settings**: Schedule automatic updates for system profile rules. See Automatic system rule updates for endpoint profiling, on page 1320.
  - **ISE Integration**: See Publish authorization attributes to Cisco ISE, on page 1292.
  - **Trust Analytics**: Click the toggle buttons to enable or disable Trust Score sources. You cannot disable the **Authentication Method** source. If an active Cisco ISE integration is configured, the authentication method used by the endpoint and its posture status will inform the Trust Score of an endpoint. You can enable or disable other sources of Trust Score data such as **AI Spoofing Detection**, Endpoint Attribute Conflict, **NAT Mode Detection**, **Concurrent MAC Addresses**, and **Security Sensor**.

    See Trust Scores for endpoints, on page 1303.
  - **Endpoint Purge Policy**: See Endpoint Purge Policies, on page 1295.
  - **Endpoint Subnet Inspection**: See Configure endpoint subnet inspection, on page 1297.

- **Endpoint MAC Randomization**

  The Endpoint MAC Randomization displays the number of static MAC addresses and random and changing MAC addresses in the network. See Trust Scores for endpoints with random and changing MAC addresses, on page 1309.

Cisco Talos Intelligence

Cisco Talos Intelligence is a comprehensive threat-detection network. Talos Intelligence comprises threat-detection analysts and real-time automated detection systems that span web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions. Integrate Cisco AI Endpoint

Analytics with Talos using the Talos IP Reputation feature to flag network connections that reach out to untrusted IP addresses, quarantine them, and protect your network from the most common cyber threats.

Catalyst Center - Cloud communicates with the Talos Intelligence Cloud Service to obtain updated IP reputation data every 30 minutes. These updates are pushed to all registered Catalyst Center devices.

There are two procedures that you can follow to set up Cisco Talos Intelligence in Catalyst Center.

Integrate Cisco AI Endpoint Analytics with Cisco Talos Intelligence through app activation

Before you begin

For the Talos IP Reputation feature to work smoothly, enable application telemetry and choose Catalyst Center as the NetFlow collector. See Configure Telemetry for more information on the NetFlow collector.

This is the recommended procedure.

Procedure

Step 1 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **External Services** > **Cisco Catalyst - Cloud**.

Step 2 From the **Region** drop-down list, choose the appropriate region.

Step 3 Scroll to the **Talos Threat Intelligence** App.

Step 4 Click **Activate** on the **Talos Threat Intelligence** App. The Cisco Cloud Services homepage displays.

Step 5 In the Cisco Cloud Services GUI, click the Menu icon, and click **Applications**.

Step 6 From the **Region** drop-down list, choose the appropriate region.

Step 7 Click **Activate** on the **Talos Threat Intelligence** App.

If the region is not selected on the **Applications** window, a **Select Region** dialog box displays. You can select the required region and then click **Activate**.

Step 8 Check the check box to agree to the terms and conditions and click **Subscribe**.

Step 9 In the **Choose Your Product** window, click Catalyst Center to choose it for Talos Threat Intelligence activation.

Step 10 In the **Activate Talos Threat Intelligence Application for your Product** window, such as **Host Name/IP**, **Name**, and **Description** (if any). Choose the appropriate type of product being registered from the **Type** drop-down list, such as Catalyst Center.

Step 11 Click **Register**.

Step 12 In the **Choose Your Product** window, click Catalyst Center to select it again and click **Select Product**.

Step 13 Click **Auto Redeem** on the **Authenticate your Product** window to automatically redeem the OTP and authenticate your product. Catalyst Center opens in a new window.

You can also copy the one-time passcode (OTP) and close the window to manually register your product.

Step 14 In the Catalyst Center window that displays, log in using your Catalyst Center credentials.

Note

- After the registration succeeds, close the window before proceeding to Cisco Cloud Services to continue with the workflow.
- After registering Catalyst Center to Cisco Cloud Services, wait for 3 minutes before proceeding to Step 15.
- In the Cisco Cloud Services GUI, (**Menu** > **Applications**), you can see the registered product with the registration status.

Step 15 Select the scopes needed for your Catalyst Center in the **Scope Selection** window and click **Next**.

A **Summary** window displays that summarizes the application, product, and scope chosen for your Catalyst Center.

Step 16 Click **Activate** to connect your Catalyst Center to Talos Threat Intelligence.

The status of the activation displays.

Step 17 Do one of these tasks:

- (If you registered your Catalyst Center device for the first time and activated Talos on Cisco Cloud Services) Click **Exit** and close the window.
- (Activated Talos for a preregistered Catalyst Center device on Cisco Cloud Services) Click **Exit** to return to the **Applications** window on Cisco Cloud Services. You can find your connected application in the **Applications** window.

Integrate Cisco AI Endpoint Analytics with Cisco Talos Intelligence using cloud authentication

Procedure

Step 1 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **External Services** > **Cloud Authentication**.

Step 2 Click the **dna.cisco.com** link and create a Catalyst Center - Cloud account.

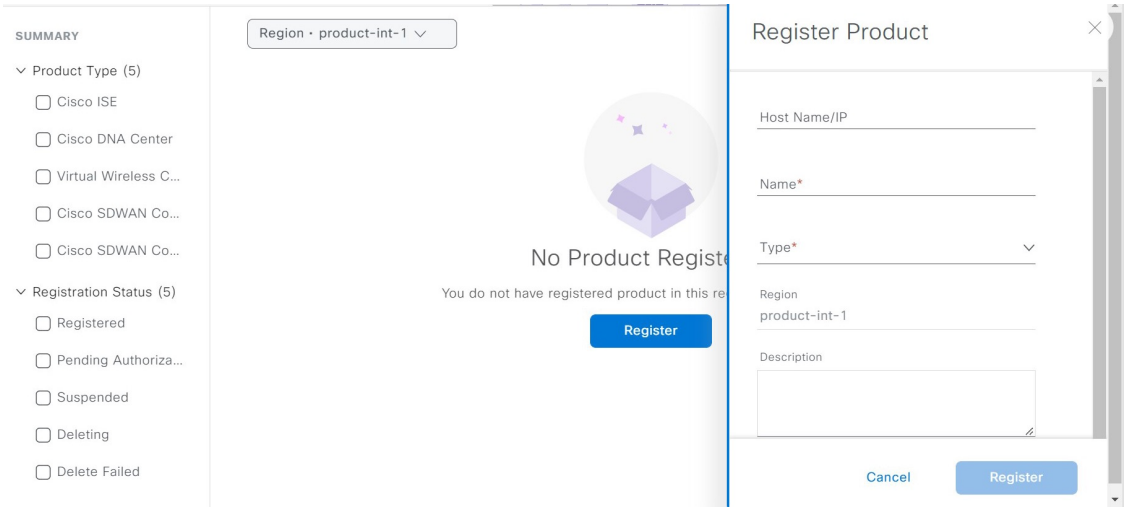
Step 3 In the Catalyst Center - Cloud GUI, click the Menu icon, click **Applications**, and choose **Products**.

Step 4 From the **Region** drop-down list, choose the appropriate region.

Step 5 Click **Register**.

Step 6 In the **Register Product** pane, enter the required details, such as **Host Name/IP**, **Name**, and **Description** (if any). Choose the appropriate type of product being registered from the **Type** drop-down list, such as Catalyst Center. Click **Register**.

Figure 34: Registering a Product to Catalyst Center - Cloud



Note Check the **Enable Cloud Access Login** check box to enable automatic login from your Catalyst Center - Cloud to Catalyst Center.

The OTP redemption occurs automatically, and Catalyst Center opens in a new window.

Step 7 In the Catalyst Center window, log in using your Catalyst Center credentials.

- After the registration succeeds, close the window before proceeding to Catalyst Center - Cloud to continue with the workflow.
- After registering Catalyst Center device to Catalyst Center - Cloud, wait for 3 minutes before proceeding to Step 8.

Step 8 In the Catalyst Center - Cloud GUI, (**Menu** > **Applications**), you can see the registered product with the registration status.

Step 9 In the Catalyst Center GUI, go to the Cisco AI Endpoint Analytics window (**AI Endpoint Analytics** > **Configurations** > **Trust Analytics**) and click the **Talos IP Reputation** toggle button to enable it. You can enable **Talos IP Reputation** from either the **Trust Score Sources** window or the **System** > **Settings** window.
After **Talos IP Reputation** is enabled, Catalyst Center receives the updated IP Reputation data whenever it's available. If an endpoint in the network tries to access an untrusted IP address, it's flagged, and a warning message stating `Detected` is displayed for Talos IP Reputation in the Trust Score view for an endpoint. This warning reduces the overall trust score of the endpoint. The Talos IP Reputation feature stores information about the untrusted IP addresses accessed and the number of access attempts made by an endpoint. This information is useful when deciding about increasing the security of your network.

The **Talos Reputation** window (**System** > **Settings** > **Talos IP Reputation**) displays the latest versions of the various files received from Talos. The time at which these files was received is also displayed. IPv4 and IPv6 files are Talos IP Reputation data files and are typically updated once a day. However, the *Threat Level* file is metadata and changes to this file are rare.

Publish authorization attributes to Cisco ISE

Publish Cisco AI Endpoint Analytics profile data to Cisco ISE to authorize endpoint access to the network and for endpoint control. The attribute information that is shared by Cisco AI Endpoint Analytics is then easily accessible to a Cisco ISE administrator through the AI Endpoint Analytics dictionary. A Cisco ISE administrator can easily create authorization policies in Cisco ISE. The attributes are shared with Cisco ISE, including:

1. The overall trust score and the score for each anomaly that is recorded.
2. CMDB attributes.
3. Multifactor profiling attributes:
    - Hardware manufacturer
    - Hardware model
    - Operating system
    - Endpoint type

If your Catalyst Center has an active integration with Cisco ISE Release 3.1 and later releases, and you want to publish authorization attributes to Cisco ISE, do these tasks.

Procedure

Step 1 To enable attribute sharing in Catalyst Center:

a) In the Cisco AI Endpoint Analytics **Overview** window, click **Configurations**.
b) Click **ISE Integration** from the left panel.
c) Click the **Enable Profile Publishing to ISE** toggle button to enable the feature.
d) Check the **Asset Topic Based Integration** or **Enhanced Authorization Integration** check boxes, or both, depending on which type of topic you want to use to publish attribute information to Cisco ISE.
e) Click **Save**.

Step 2 To enable pxGrid subscription in Cisco ISE:

a) In the Cisco ISE GUI, click the menu icon and choose **Work Center** > **Profiler** > **Settings**.
b) If you are connected to Cisco ISE Release 3.1, in the **Endpoint Analytics Settings** area, check these check boxes:
    - **Publish Endpoint Attributes to AI Endpoint Analytics**
    - **Consume Endpoint Profiles from AI Endpoint Analytics**

What to do next

To verify the subscription, from the Cisco ISE main menu, do this:

- For Cisco ISE 3.1: Choose **Administration** > **pxGrid Services** > **Diagnostics** > **WebSocket** > **Clients**
- For releases later than Cisco ISE 3.1: Choose **Administration** > **pxGrid Services** > **Diagnostics** > **Connections** > **Clients**

The newly created subscription containing "com.cisco.ea.data.ise-<Cisco ISE node>" displays in the **Subscription** column of the PSN nodes.

In the Cisco ISE **Policy** > **Policy Sets** window, a new dictionary that is named **Endpoint-Analytics** is visible in the Conditions Studio.

In the Cisco ISE **Context Visibility** > **Endpoints** window, click **MAC Address** for endpoint details. The attributes area of the details displays attributes that contain "EA-" prefixes for the attributes that are received from Cisco AI Endpoint Analytics.

Trust Analytics

The **Trust Analytics** window displays the various trust score sources, enables you to reset alerts raised on these sources manually or automatically after a period of inactivity, and sets the impact level for each trust score source to accurately measure the overall trust score of an endpoint.

Trust Score assesses the trustworthiness of a given endpoint on the network to help achieve zero trust outcomes. Values range from 1 (low trust) to 10 (high trust) and are calculated using several sources:

- **Endpoint Context**: This category of sources provides information about the reliability of an endpoint, by knowing the authentication method used by the endpoint and posture status of the endpoint.
- **Threat and vulnerability Context**: This category of sources provides information about how vulnerable an endpoint is based on the various types of threats associated with an endpoint.
- **Network Context**: This category of sources provides information about how an endpoint is accessing the network.

Trust Score Impact allows you to control the trust score of an endpoint when an anomaly is raised. These impact levels are available:

- **Low**: When you know that an anomaly is of low importance in your network, you can set its impact level to **Low** so that it has a low impact on the trust score. After setting this impact level, when such an anomaly is detected again, the trust score for the endpoint on which the anomaly is detected sluggishly reduces to 1 (Increases system-generated impact level by 50% of total trust score).
- **Critical**: When you know that an anomaly is of high importance in your network, you can set its impact level to **Critical** so that it has a very high impact on the trust score. After setting this impact level, when such an anomaly is detected again, the trust score for the endpoint on which the anomaly is detected quickly reduces to 1 (Reduces system-generated impact level by 50% of total trust score).
- **No Impact**: An anomaly is detected, but does not impact the overall trust score. You can use this option to test out the anomalies and view them without changing the overall trust score.
- **System Default**: Default system-generated trust score.

To know how to customize impact levels for the sources, see Customize Impact Level.

Alerts appear when there is a deviation caused by anomalies or vulnerabilities, or when a weakness is identified in endpoint connections or interfaces. The alerts can be reset manually after addressing them. You can also manually reset the alerts you don't want to address. Alternatively, you can set a reset timer to reset the alerts automatically. After a period of inactivity, this alert is not detected on endpoints.

To know how to reset alerts for the sources, see Reset Alert.

Customize impact level

You can now customize the trust score of an endpoint by setting an impact level that you perceive for an endpoint. Based on the impact level that you set for a source, the overall trust score is recalculated for the endpoints. This gives you the authority to decide the trust level of an anomaly irrespective of the system-generated trust score for that anomaly.

Note For authentication method EAT-TLS and posture non-compliant endpoints, even if you change the impact level, the trust level remains the same. The trust level is only changed in the case of MAB authentication.

Note The high trust score that is earned because of the authentication method used, is not lowered even when the impact level for the authentication method is changed. If the impact level for the authentication method is increased, the endpoints continue to retain their current trust score unless a new session for that endpoint is received.

Procedure

Step 1 From the main menu, choose **Policy** > **AI Endpoint Analytics** > **Overview** > **Manage Sources**.
The **Trust Analytics** window opens.

Step 2 Click **Customize Impact Level**.

Step 3 Click **Let's Do It**.
The **Customize Trust Score Sources** workflow begins. You can exit the workflow at any point in time by clicking the **Exit** option at the bottom of the workflow window.

Step 4 Check the checkboxes next to the sources for which you want to change the impact level.

Step 5 From the **More Actions** drop-down list, choose the **New Impact Level**.

Step 6 Click **Next**.

In the next window, a comparative study of the previous and new trust score is provided that shows the trust score customization impact on individual endpoints. This pie chart includes all the endpoints in the network irrespective of whether or not they were impacted by the change in the impact level of the sources. The **Endpoints (After)** table below displays the new trust score for each endpoint that was impacted as a result of the change in the impact level configuration.

Step 7 Click **Next**.

A summary stating the new impact level of each source is displayed. Click **Edit** to go back in the workflow to edit the impact level of the trust scores in case you are not satisfied with the result.

Step 8 Click **Next**.

The endpoints' trust scores are updated accordingly and is also sent to Cisco ISE. This may result in a change of authorization for such endpoints if Cisco ISE is using trust score based authorization policies.

What to do next

Check the new trust score for the endpoints in **Policy** > **AI Endpoint Analytics** > **Trust Score**.

Configure reset alert

You can reset an alert manually or automatically after a period of inactivity. By default, the reset action is set to **Manual** for all supported sources. You can configure to reset an alert using the global configuration workflow as described here.

Procedure

Step 1 From the main menu, choose **Policy** > **AI Endpoint Analytics** > **Manage Sources**.

The **Trust Analytics** window opens.

Step 2 Click **Alert Configuration**.

Step 3 In the **Choose Reset Alert Type** window, click **Let's Do It**.

You can exit the workflow at any point in time by clicking the **Exit** option at the bottom of the workflow window.

Step 4 From the **Reset Alert Type** drop-down list, choose **Manual** or **Customize reset timer after alert inactivity**.

Step 5 If you choose **Customize reset timer after alert inactivity**, enter the number of days (0 to 365 days) or hours (0 to 24 hours), after which you want to reset the alert, in case of inactivity.

You can choose to remove or retain the ANC Policy. If the endpoint has a trust value from more than one trust score source, the ANC policy will not be removed even if the **Remove ANC Policy** checkbox is checked.

Step 6 Click **Next**.

Step 7 Check the check boxes next to all the sources for which you want to apply the setting that you chose in Step 4.

Step 8 Click **Apply**.

You can also configure to reset an alert locally from the **Trust Analytics** window. Choose the source for which you want to configure the reset alert. In the slide-in window on the right, choose the appropriate setting and click **Save**.

Note The reset alert configuration option is not available for all sources. When the alerts are reset, the same information is propagated back to Cisco ISE.

The alerts are checked every 30 minutes for an update. And if, during any of the checks, the time period configured in the reset alert configuration has lapsed, the trust score is reset for that anomaly. The status of the reset alert will be displayed in the Audit log.

Endpoint Purge Policies

Define an Endpoint Purge Policy to remove from your network the endpoints that have been inactive for a defined time. You can define the period of inactivity after which an endpoint must be removed. You can also customize a purge policy to act on a particular set of endpoints based on a profiling attribute. Purge policies

are executed at 2 A.M. (server time) every day, and the endpoints that meet the defined purge requirements are removed from your network.

Registered endpoints and static endpoints that are imported into Cisco AI Endpoint Analytics are not affected by endpoint purge policies.

The Backup and Restore operation in your Catalyst Center and the endpoint purge activity cannot run simultaneously. If a Backup and Restore operation is in progress at 2 A.M., the purge activity is not initiated. If a Backup and Restore operation starts while an endpoint activity is in progress, the endpoint purge stops running, and the purge activity is left incomplete. The remaining endpoints are not acted on until the next purge is executed at 2 A.M. (server time) the next day.

To view, edit, or add endpoint purge policies, click the menu icon and choose **Policy** > **AI Endpoint Analytics** > **Configurations** > **Endpoint Purge Policy**. The following policies are available by default:

- **Default**
- **Random MAC Default**

You cannot edit these default policies. You can only enable or disable them.

You can use the **Purge Now** option to immediately run the purge policy instead of waiting until 2 AM. There are two ways to use the **Purge Now** option:

- Choose the purge policies that you want to run now and from the **More Actions** drop-down list, choose **Purge Now**.
- Click the icon under the **Actions** column for the purge policy that you want to run now and choose **Purge Now**.

Create a Purge Policy

Procedure

Step 1 From the main menu, choose **Policy** > **AI Endpoint Analytics** > **Configurations** > **Endpoint Purge Policy**.

Step 2 Click **Add Endpoint Purge Policy**.

Step 3 In the **Add Endpoint Purge Policy** dialog box, click **Let's Do It** to go directly to the workflow.

Step 4 In the **Define Policy Details** window, do these steps:

a. Enter a name for your policy in the **Rule Name** field.

b. From the **Select Status** drop-down list, choose **Enabled** or **Disabled**.

c. Define the time of inactivity after which an endpoint must be purged. Enter a value (in days) in the **Elapsed Greater than or Equal to** field. The accepted value range is from 5 to 180 days.

Step 5 (Optional) In the **Define Additional Policy Conditions** window, choose the profiling attributes, to filter the endpoints that are impacted by this purge policy. Check the check box next to the attribute you want to select and choose the required values from the drop-down lists displayed for the attribute.

Step 6 The **Summary** window displays your Purge Policy configuration. Review the details that are displayed and click **Done** to create the policy.

What to do next

Audit Logs of Endpoint Purge Activities

After you enable an Endpoint Purge Policy and a purge activity is executed, you can view the audit logs. For more information, see **View Audit Logs** in the Cisco Catalyst Center Administrator Guide.

Configure endpoint subnet inspection

In a deployment, devices at the access layer and devices above the access layer have different IP subnets. In the case of Cisco TTA devices, endpoint profiling accuracy is optimum when only southbound traffic is analyzed by Cisco AI Endpoint Analytics. To allow better endpoint profiling, configure specific IP subnets or subnet ranges that must be analyzed by Cisco AI Endpoint Analytics.

This configuration of filtered subnets is then shared with Cisco SD-AVC servers. The configuration is applied on Cisco TTA devices though Cisco SD-AVC servers.

Procedure

Step 1 From the main menu, choose **Policy** > **AI Endpoint Analytics** > **Configurations** > **Endpoint Subnet Inspection**.

Step 2 Enter the required value in the **IP Subnet** field.

Step 3 Click + to add another IP subnet. You can add multiple subnets or subnet ranges in this window.

Endpoint Inventory

The **Endpoint Inventory** tab displays details of the endpoints that are connected to Cisco AI Endpoint Analytics through the configured data sources. This view displays the profiling information of all the connected endpoints.

To select the profiling information you want to view for the endpoints, click the vertical ellipsis icon at the top-right corner of the table. Select one of these sets of profiling information and click **Apply**:

- **All**: All the profiling information that is available is displayed. You cannot edit this set.
- **General**: This is a selection of profiling information that gives you a generic view of the endpoints. This is the set of columns that are displayed by default. You cannot edit this set.
- **Detailed**: This is a selection of profiling information that provides a deeper view of the endpoints. You cannot edit this set.
- **Custom**: This is the only set that you can edit. Check or uncheck the profiling information that you want to view in the **Endpoint Inventory** window.

You can also filter the list endpoints that is displayed in the **All Endpoints** view by clicking the required **View Known Profiles** buttons. You can filter the list of endpoints by **Endpoint Type**, **Hardware Manufacturer**, **Hardware Model,** and **OS Type**.

To edit or customize the endpoint inventory table that is displayed, click the gear icon in the right corner at the top of the table. The pane that is displayed contains the **Table Appearance**, **Edit Table Columns**, and

Edit Custom Views menus where you can select a table view, the information that you want displayed in the table, and create custom views.

Click **Apply** to save the changes, or click **Reset All Settings** to apply the default settings for the endpoint inventory table.

You can easily filter a set of endpoints based on your requirement. The search bar at the top of table allows you to easily find a filter parameter. You can type and use the assisted search feature, or you can scroll the drop-down that is displayed to find and select the required parameters.

Most of the columns contain quick filters. While some filters display drop-down menus for you to select values from, some filters are text fields you can type into.

You can register endpoints, and edit, delete, and profile the registered endpoints. You can select single or multiple endpoints by checking the check box near the MAC addresses to filter and perform a particular action on the chosen endpoints from the **Actions** drop-down list.

You can delete registered endpoints, unregistered endpoints, and endpoints learned from other sources. When you select an endpoint, a banner row is displayed that allows you to select all the rows in the table. When you click the banner, the banner row now allows you to clear all the rows in the table. To delete all the endpoints, you can click the banner or select the **Delete** option from the **More Actions** drop-down list.

To see the complete profiling details of an endpoint, click the **MAC Address** of the endpoint. A slide-in dialog box is displayed which contains user details, endpoint details, and attribute details of the endpoint.

In the **Details** tab, these fields display the details received from Cisco ISE:

- **Authentication Status**: This field displays **Started** when an endpoint is authenticated through Cisco ISE, and **Disconnected** when it is not.
- **Authorization Profile**: The authorization policies configured for an endpoint in Cisco ISE are displayed here.
- **Security Group Tag**: The Security Group Tags configured for an endpoint in Cisco ISE are displayed here.

For information on these attributes, see the Cisco ISE Administrator Guide for the Cisco ISE release that you use.

The **Trust Score** tab is available in the slide-in dialog box for endpoint details. This tab displays details of the various factors that inform trust score of an endpoint. See Trust Scores for endpoints, on page 1303.

The **Details** tab contains the **Previous MAC Addresses** area, which displays the MAC addresses that have been used by an endpoint that has the MAC Randomization feature enabled on it. See Trust Scores for endpoints with random and changing MAC addresses, on page 1309.

Export Cisco AI Endpoint Analytics data

To export a list of endpoints and their details from this window, click **Export**. If you apply any filters in the **Endpoint Inventory** window, only the filtered endpoints will be processed for export. To export the details of all the endpoints, ensure that no filters are applied when you click **Export**.

When you click **Export**, a new tab opens with the **Reports** window. The **Generated Reports** window contains a list of exports initiated, with the latest export request at the top of the list. A report generated from the **Endpoint Inventory** window contains **AI Endpoint Analytics** in its **Template Category** column. Report generation takes a few minutes. When a report is ready for download, the value in the **Last Run** column changes from **Not Initiated** to a timestamp with a download icon next to it. The timestamp refers to the time

at which the export list was generated. Click the download icon to download a CSV file of the list of endpoints to your system.

You can also export Cisco AI Endpoint Analytics data from the **Reports** window, through these steps:



Note You must run your first export of AI Endpoint Analytics data for endpoints from the **Endpoint Inventory** window. Then you can generate AI Endpoint Analytics reports directly from the **Reports** window.

Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates** > **AI Endpoint Analytics**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.



Note To skip this screen in the future, check the **Don't show this to me again** check box.

Step 3 In the **Select Report Template** window, the template **Endpoint Profiling** applies by default.

Step 4 In the **Setup Report Scope** window, do these steps:

a) Enter a name in the **Report Name** field.

b) Define the filters that you want to apply to the list of endpoints that you want to export from the **Endpoint Inventory** window.

c) To export the details of all endpoints, do not choose any values in the **Scope** area.

Step 5 In the **Select File Type** window, the **Client Details** area allows you to review the chosen parameters. Edit the information to be exported by checking or unchecking the check boxes next to the relevant fields.

Step 6 In the **Schedule Report** window, click **Run Now**, **Run Later (One-Time)**, or **Run Recurring** radio button.



Note The **Run Later (One-Time)** and **Run Recurring** options display scheduling fields to define the time of export.

Step 7 In the **Delivery and Notification** window, do not check the **Email Report** check box.

Step 8 In the **Summary** window, review all the configurations. To make any changes, click **Edit**.

Step 9 Click the **View Reports** link in this window for a list of generated reports. It takes a few minutes for the report to generate and display in this window.

Filter endpoints

Use this procedure to filter endpoints based on their profiling data, primary profiling labels, known profiles, and health status.

Procedure

Step 1 In the **Endpoint Inventory** window, click **Filter**.

Step 2 Define these filters by choosing a value from the corresponding drop-down list, clicking the radio button for the required value, or checking the check box next to the required value for a particular field, as applicable:

- **Profile Status Condition**
- **Mac Address**
- **Is Random Mac**
- **Trust Score**
- **IP Address**
- **Last Seen**
- **Host Name**
- **Endpoint Type**
- **OS Type**
- **Hardware Model**
- **Hardware Manufacturer**
- **Registered**

Step 3 Click **Apply**.

You can also filter the profiled endpoints displayed by the four primary profiling labels. Click one or more of the labels in the **View Known Profiles** section.

The health status of endpoints is updated every 5 minutes.

Attribute Glossary

Attribute glossary is a list of all the profiling attributes available from Cisco ISE probe data.

Use this procedure to view all the profiling attributes.

Procedure

Step 1 In the **Endpoint Inventory** window, click the MAC address of an endpoint.

Step 2 In the new area that is displayed on the right side, click **View Attribute Glossary**.

The **Attribute Glossary** window displays information for each attribute, including:

- **Key profiling attributes**

- **Description**
- **Associated Profile Labels**
- **Source**
- **Dictionary**
- **Discovery Method**

The glossary gives you a detailed view of all the profiling attributes. If a profiling attribute is frequently used to create a profile label, the label is listed in the **Associated Profile Labels** column.

You can also view the attribute glossary in the **Choose Attribute Condition** window while creating a logical condition for the rules. For more information, see Create a Custom Rule.

Register endpoints

You can onboard and profile new endpoints by registering them in Cisco AI Endpoint Analytics. The profiling information of an endpoint is the source of truth for classification. You can also update new profile information for a registered endpoint using the **Register Endpoint** option.

Procedure

Step 1 Choose **Actions** > **Register Endpoints**.

Step 2 Select whether you want to register a single endpoint or multiple endpoints, by clicking the **Single** or **Bulk** radio button.

a) Click **Single** radio button, enter the **MAC Address**, **Endpoint Type**, **Hardware Model** and **Hardware Manufacturer** for the endpoint.

b) Click **Bulk** radio button and do these steps:

1. Download a .csv template by clicking the **Download .csv Template** option.
2. In the downloaded .csv file, enter these details for each endpoint you must register: MAC address, endpoint type, hardware model, and hardware manufacturer. Save this file.
3. Upload the .csv file using the **Choose a File** option.

You can register a maximum of 500 endpoints at a time using the **Bulk** option.

Step 3 In the **Review Endpoint** window, review the endpoint details. To make any changes, click **Edit**.

Note While registering an existing endpoint, the profile label changes of the endpoint are reflected in purple color and can be edited.

Step 4 Click **Next** to continue with the registration process.

Step 5 Click **Register**.

Edit registered endpoints

You can update the profiling information of registered endpoints from the **Endpoint Inventory** window.

Procedure

Step 1 Check the check box adjacent to the MAC address of the endpoint that you want to edit.
Step 2 Click **Actions**.
Step 3 Click **Edit Endpoint**.
Step 4 Enter the **Endpoint Type**, **Hardware Model**, and **Hardware Manufacturer** details.
Step 5 Click **Save**.

Delete registered endpoints

If there are registered endpoints that are no a longer part of your network, you can delete them from Cisco AI Endpoint Analytics.

Procedure

Step 1 Check the check box adjacent to the MAC address of the endpoints that you want to delete.
Step 2 Click **Actions**.
Step 3 Click **Delete Endpoint**.

This message displays:

```
Do you really want to delete the selected endpoint(s)?
```

Step 4 Click **Yes** to permanently delete the endpoint from Cisco AI Endpoint Analytics.

Trust Score

The **Trust Score** window consists of two tabular sections:

Alerts:

Alerts appear when there is a deviation caused by anomalies or vulnerabilities, or when a weakness is identified in endpoint connections or interfaces. These alerts reflect a detection that has a negative impact on the trust score (such as concurrent MAC address detection, NAT mode, or other untrustworthy changes). You can monitor the alerts to quickly address the most urgent risks within your network.

The **Alerts** tab displays the various alerts received by the endpoints in the network. Earlier you had to individually check the details for each endpoint to see the type of alerts the endpoint has received and there was no way to know what other endpoints have received the same alert. Now, you have the capability to know all the endpoints that have received a particular type of alert. You can click on any alert to view the list of endpoints that have received this alert. You can further click on each endpoint to see the details. The alerts can be in any of these three states:

- **Open**: An alert is in the open state when the alert is initially detected for an endpoint and an action is required from your side to resolve the alert or address it later.
- **Disabled**: If you do not want to take any action on an open alert, you can move it to the disabled state. You can disable the alert for any time period and even indefinitely. During this time period, the alert remains in the disabled state even if any new endpoints are detected with this alert.
- **Reset**: If you do not want to take any action on an alert right away, you can move it to the reset state. When this alert is detected on another endpoint after resetting, the alert is brought back to the open state.

Endpoint:

This view displays columns for the various factors that inform the overall Trust Score of an endpoint. The Trust Score helps you identify the endpoints in which behavioral anomalies have been detected, so you can examine the details of the endpoint and take the necessary remediation actions. If you apply an ANC policy to an endpoint to manage its low Trust Score, the Trust Score view also displays the name of the ANC policy applied and when the policy was applied. See Trust Scores for endpoints, on page 1303.

Using the option **Reset Trust Score**, you can now reset multiple endpoints at the same time with an upper limit of 10 endpoints to avoid any performance issues. While resetting the endpoints, a justification is required for the action for audit purposes. After an endpoint is reset, the endpoint is cleared of its Trust Score and any ANC policy that was applied to it.

Trust Scores for endpoints

Cisco AI Endpoint Analytics assigns Trust Scores to endpoints to allow you to easily monitor and act on potentially risky endpoints in your network. Behavioral anomalies are monitored and tracked, and a Trust Score is assigned based on the number and frequency of the anomalies tracked.

To select the sources that must be included in the calculation of Trust Scores, from the Cisco AI Endpoint Analytics **Overview** window, choose **Configuration** > **Trust Analytics**. Click a source to open its slide-in configuration window on the right. Click the toggle button to enable the source.

Cisco AI Endpoint Analytics generates historical Trust Scores based on these factors:

- The history of anomalies associated with an endpoint—how many anomalies have been detected for this endpoint?
- The severity of each anomaly detected for the endpoint.

The overall Trust Score calculation for an endpoint factors in these anomalies and scores display for each anomaly that is detected (if the corresponding source is enabled):

- **AI Spoofing Detection**

  Cisco AI Endpoint Analytics analyzes NetFlow telemetry data, and network probe data from Cisco ISE and SD-AVC devices, to detect spoofed endpoints. For more information on how to configure NetFlow Collector servers, see Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry, on page 43. Probe and NetFlow data from Catalyst Center Traffic Telemetry

Appliances (DN-APL-TTA-M) is also analyzed. Configure inbound span of traffic toward your Catalyst Center Traffic Telemetry Appliances so the endpoint traffic data is then available to Cisco AI Endpoint Analytics for spoofing detection.

Each endpoint type has a behavior model that is developed using machine learning algorithms. Based on the data received for an endpoint, if an endpoint's behavior is unexpected of its endpoint type profile, the endpoint is assigned a low Trust Score in the AI Spoofing Detection area. The applications and server ports that are used by an endpoint are analyzed in this spoofing detection process. For example, if an endpoint profiled as a printer uses a video calling application, it is identified as a spoofed endpoint and assigned a Trust Score.

Endpoints are identified by their MAC addresses on a Catalyst Center-managed switch. Several endpoints using a single MAC address such as by using NAT, running a virtual machine or a container, is not a supported configuration on Cisco AI Endpoint Analytics.

AI Spoofing Detection covers these device types:

- IP Phones
- Printers
- Cameras
- Building automation devices with these hardware model attributes:
    - Automated-Logic-Device
    - Honeywell-Device
    - Johnson-Controls-Device
    - Rockwell-Automation-Device
    - Schneider-Electric-Device
    - Siemens-Automation-Device
    - Siemens-Building-Device
    - Trane-Device
- Telepresence:
    - Endpoints with one of these hardware models:
        - Cisco-Tandberg-Device
        - Cisco-TelePresence
        - Cisco Telepresence SX80
        - Cisco Telepresence SX20
        - Cisco-Collaboration-Room-Endpoint
        - Poly-Device
    - Endpoints with the device type Video Conferencing

- **Endpoint Attribute Conflict**

When a device joins a network, and then through periodic probing while the device is active, the profiling data for an endpoint is continuously monitored and updated. Certain changes in the profiling data that is received from an endpoint are flagged as anomalies in Cisco AI Endpoint Analytics. For example, if an endpoint was first profiled as a Linux device and is then profiled as a macOS device, this is flagged as a high-severity anomaly. A score is assigned in the Endpoint Attribute Conflict column for the endpoint and the endpoint's overall Trust Score is also updated to reflect this change.

However, if there is a change in the version of macOS and the endpoint appears to have downgraded from a later release to an earlier release, such a change is flagged as a lower priority anomaly and the corresponding scores are updated accordingly.

- **NAT Mode Detection**

  If you have a NAT-enabled router in your network, an endpoint that is connected to a NAT router is recognized by the IP or MAC addresses of the router instead of the IP or MAC addresses of the specific endpoint. Information on NAT-enabled routers is collected from the Cisco Catalyst 9000 Series devices they are connected to.

- **Concurrent MAC Addresses**

  Identify the endpoints that share the same MAC addresses and are connected to Cisco Catalyst 9000 Series devices. The endpoints with shared MAC addresses are assigned a Concurrent MAC Address score, and you can easily identify these endpoints and examine their details.

- **Security Sensor**

  With the Security Sensor scan feature, you can install active probes on specific Cisco Catalyst 9000 Series switches, and configure Cisco AI Endpoint Analytics to scan endpoints for open ports that are not expected to be open, for credential vulnerabilities or both.

The Trust Score of an endpoint is also informed by the events that are collected from Cisco ISE. Every endpoint that authenticates through Cisco ISE receives an initial Trust Score based on these events:

- **Authentication Method**
- **Posture**

Note For the Trust Score sources that receive data from Cisco Catalyst 9000 Series devices, you must enable CBAR on the devices and upgrade the devices to Cisco IOS-XE Release 17.6 or later.

The Trust Score that displays in the **Endpoint Inventory** window is the overall trust score that takes the history and severity of anomalies for an endpoint. Click the **MAC Address** to view the details of the causes for the Trust Score that is assigned to an endpoint. This means that if a low-level anomaly was detected for an endpoint, and this is the only instance of an anomaly, the overall Trust Score for the endpoint would be a 9.

If multiple low-level anomalies are detected, the overall Trust Score would further decrease to account for the number of anomalies.

The trust scores assigned range from 1 through 10, and are categorized in this table:

Trust Score category	Range	Threat level of endpoint
Low	1–3	High

Trust Score category	Range	Threat level of endpoint
Medium	4–6	Moderate
High	7–10	Low

You can then apply Adaptive Network Control (ANC) policies from Cisco ISE to enforce appropriate remediation actions on the endpoints. See section "Adaptive Network Control" in Chapter "Cisco ISE Admin Guide: Maintain and Monitor" of the *Cisco ISE Administrator Guide*.

The ANC policies are defined in Cisco ISE and allow you to apply remediation actions on chosen endpoints. You can apply ANC policies to quarantine, shut down, or port bounce an endpoint, or force endpoint reauthentication. When you apply an ANC policy to an endpoint with an undesirable Trust Score in Cisco AI Endpoint Analytics, a Change of Authorization (CoA) is sent to the endpoint from Cisco ISE.

An endpoint is identified by its MAC address. Cisco ISE sends the CoA to the endpoints that hold an active session for the identified MAC address at the time of the ANC application. Any endpoint with the same MAC address that does not have an active session in Cisco ISE at the time matches the ANC policy when a new session starts or when it must reauthenticate at the end of the configured reauthentication timer.

To verify which endpoint is being acted upon by the ANC policy, log in to your Cisco ISE administration portal. From the main menu, choose **Operations** > **RADIUS** > **Live Sessions**. Enter the MAC address of the spoofed endpoint in the **Endpoint ID** column, to filter the endpoints that share the same MAC address and currently have live sessions in Cisco ISE. These are the endpoints that will be affected by the ANC policy.

To view a historic log of the RADIUS sessions in Cisco ISE, from the main menu, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **RADIUS Authentications**.

To view or modify ANC policy application on endpoints in Cisco ISE, from the main menu, choose **Context Visibility** > **Endpoints**. Check the check box next to the MAC address of an endpoint and click the options that are displayed at the top of the list, as required.

Prerequisites

Prerequisites for receiving Trust Scores for endpoints:

- Cisco ISE is connected to your on-premises Catalyst Center.
- Network access devices are managed by both Cisco Catalyst Assurance and Cisco ISE.

Note The endpoint spoofing detection feature supports a maximum of 500 network access devices with NetFlow export flows, as Cisco Catalyst Assurance supports only 500 NetFlow exporters.

- Endpoints connected to network access devices are authenticated through Cisco ISE.
- Enable the required sources for Trust Score calculation in the Trust Score Sources window (**Policy** > **AI Endpoint Analytics** > **Configurations** > **Trust Analytics**).

Endpoint Attribute Conflict

Cisco AI Endpoint Analytics collects data from multiple probes from different sources continually to derive accurate profile labels for endpoints. Cisco AI Endpoint Analytics collects this data from these sources:

From Cisco ISE:

- RADIUS probes.
- User details from Directory.
- VPN details like AnyConnect availability.
- Optionally, other data if port forwarding is configured. For example, DHCP details.

From switches:

- Device connection messages. For example, DHCP and NetBIOS messages.
- Deep packet inspection
- Switch telemetry

Cisco AI Endpoint Analytics creates system rules based on the information received from these sources. When a device joins a network, and then through periodic probing while the device is active, the profiling data for an endpoint is continuously monitored and updated.

Certain changes in the profiling data received from the endpoint are flagged as anomalies in Cisco AI Endpoint Analytics. For example, if an endpoint was first profiled as a Linux device and is then profiled as a macOS device, this is flagged as a high-severity anomaly. A score is assigned in the Endpoint Attribute Conflict column for the endpoint and the endpoint's overall Trust Score is also updated to reflect this change.

However, if there is a change in the sub-version of macOS and the endpoint appears to have downgraded from a later release to an earlier release, such a change is flagged as a lower priority anomaly and the corresponding scores are updated accordingly.

In the **Endpoint Inventory** window, click the MAC Address of an endpoint with a **Endpoint Attribute Conflict** score to view the profiling data changes recorded. The old and new profiles for the endpoints are displayed here. If the profiling changes are not of concern for any reason, or if you think the profiling change detected is erroneous, reset the score by clicking the corresponding button in the **Endpoint Attribute Conflict** area of the endpoint's details.

You can also disable Endpoint Attribute Conflict detection for a specific endpoint by clicking the toggle button in the Endpoint Attribute Conflict area of the endpoint's details.

Data regarding this anomaly is sent to Cisco ISE if the affected endpoint is connected to Cisco ISE. The data is available as an Endpoint Analytics dictionary attribute that a Cisco ISE administrator can easily use to define policies.

Endpoint Attribute Conflict detection is not available for the endpoints that have Custom Rules applied to them.

NAT Mode Detection

Network Address Translation (NAT) allows private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT can be configured to advertise to the outside world only one address for the entire network. If you have a NAT-enabled router in your network, an endpoint connected to a NAT router is recognized by the IP or MAC addresses of the router instead of the IP or MAC addresses of the specific endpoint. Information on NAT-enabled routers is collected from the Cisco Catalyst 9000 Series devices they are connected to.

NAT detection is included in Trust Score calculation as a device acting as a NAC-enabled router could allow unauthorized endpoints to connect to your network. For the endpoints that are assigned a NAT Mode Detection

score, in the **Endpoint Inventory** tab, click the MAC Address to view the details of the endpoint in a slide-in window. If you are certain that the identity of the endpoint corresponds to a NAT-enabled router in your network:

1. Click **NAT Mode Detection** in the **Trust Score** tab of the details slide-in window.
2. Click the toggle button to disable NAT Detection for this specific endpoint.

Endpoints with concurrent MAC addresses connected to Cisco Catalyst 9000 Series devices

Identify the endpoints that share the same MAC addresses and are connected to Cisco Catalyst 9000 Series devices. The issue of endpoints with concurrent MAC addresses occurs in wired environments and in hybrid environments that contain wired and wireless deployments. In a wireless environment, concurrent MAC addresses do not occur as only one endpoint with a specific MAC address is allowed to access the network at any time.

Cisco AI Endpoint Analytics allows you to identify the endpoints with concurrent MAC addresses by assigning a Concurrent MAC Address score to the endpoints. To detect endpoints with shared MAC addresses in your network, you must enable CBAR in the connected Cisco Catalyst 9000 Series devices.

When devices with the same MAC Address connect to a Cisco Catalyst 9000 Series device, the endpoints are recognized as concurrent endpoints and a low score is assigned to the MAC Address. Endpoints with concurrent MAC addresses may be connected to:

- The same Cisco Catalyst 9000 Series device from different VLANs
- Different Cisco Catalyst 9000 Series devices

Table 73: Environments in which the concurrent MAC address issue occurs

Deployment 1	Deployment 2	Can concurrent MAC addresses occur in the network?	Concurrent MAC addresses detection support in this environment
Wired	Wired	Yes	Yes
Wired	Wireless	Yes	Yes
Wireless	Wired	Yes	Yes
Wireless	Wireless	No	No

The **Trust Scores** view of the **Endpoint Inventory** tab contains the **Concurrent MAC Address** column. Shared MAC addresses are detected as an anomaly and a low score is assigned in the **Concurrent MAC Address** column. Click the MAC Address to view a slide-in window with the details of the MAC Address. Click **Concurrent MAC Address** and the field expands to display information regarding the various sources of the MAC address.

In the **Concurrent MAC Address** area, the **Network Device Name** column displays the name of the Cisco Catalyst 9000 Series device to which an endpoint is connected. The **Interface** and **VLAN** columns display the corresponding values to help you identify how the endpoint is connected to the network.

Initial Trust Score assessment using Posture and authentication values from Cisco ISE

When an endpoint authenticates through Cisco ISE, a Trust Score is immediately assigned to the endpoint based on its authentication and posture details. Authentication Method score is assigned by default and you

cannot disable or act upon this score. You can choose to enable or disable Posture-based scores, either at a global level from the **Configurations** window, or for a particular endpoint in the **Endpoint Inventory** tab. The Trust Score that is assigned based on the Authentication Method and Posture values becomes the initial Trust Score for the endpoint.

Any other anomalous behaviors detected for this endpoint would then impact this initial Trust Score and drive it lower based on the severity and number of the anomalies.

The **Authentication Method** score, displayed in the details of an endpoint in the **Endpoint Inventory** tab, is based on the perceived security level of the authentication method used. For example, WebAuth Over HTTPS, certificate-based authentication, and authentication using secure tunnels receive high Trust Scores.

The **Posture** score is based on whether or not the connect endpoint is posture compliant.

If an endpoint's Trust Score consists of only the Authentication Method score, the **Reset Trust Score** button is inactive. When a Trust Score source other than the Authentication Method displays a score, you can use the reset option.

Trust Scores for endpoints with random and changing MAC addresses

As a privacy measure, mobile devices increasingly use random and changing MAC addresses for each SSID that they connect to. Some desktop operating systems offer users the ability to randomize MAC addresses at regular intervals as well. This means that an endpoint presents different MAC addresses every time they connect to a different SSID.

Cisco AI Endpoint Analytics enables you to handle the issue of random and changing MAC addresses by receiving from Cisco ISE a unique endpoint identifier called the DUID (also known as GUID in Cisco ISE). Cisco AI Endpoint Analytics then uses the DUID as the identifier for an endpoint, instead of its MAC address.

The Endpoint MAC Randomization dashlet in the Cisco AI Endpoint Analytics **Overview** window displays a graphical representation of how many endpoints in your network are using random and changing MAC addresses.

For the endpoints that are connected to Cisco ISE and have DUID information available, this information is displayed in Cisco AI Endpoint Analytics as well. These columns display the required information in the **Endpoint Inventory** window in Cisco AI Endpoint Analytics:

- **DUID**: The DUID value for the endpoint.
- **Previous MAC Addresses**: The random and changing MAC addresses with which the endpoint previously connected to the network.

Using the DUID value, Cisco AI Endpoint Analytics is now able to reliably identify an endpoint and track the various MAC addresses that the endpoint has previously used. This means that the Trust Score for an endpoint with random and changing MAC addresses still has high fidelity. The Trust Score of the endpoint from a previous MAC addresses is carried forward to the current MAC address that the endpoint is presenting and continues to be impacted by the probe data received for the same endpoint.

If a device has the **Private Address** setting enabled, the **Is MAC Random** column for this device displays the value **Yes**. This device is then recognized as a random and changing MAC address. However, whether or not a DUID value is available for this device depends on whether or not the endpoint was authenticated through Cisco ISE and if a GUID was generated for this endpoint in Cisco ISE.

Sensor scans to check for open ports and credential vulnerabilities

Install an active probes container to gain more information about the endpoints in your network. When you enable security sensor scans, the Trust Score that is assigned to an endpoint takes into account any anomalies in open ports and endpoint login credentials.

The sensor scan feature is supported by these switches:

- Cisco Catalyst 9300 Series switches
- Cisco Catalyst 9400 Series switches

Note Cisco Catalyst 9800 Series Wireless Controllers do not support the sensor scan feature.

Cisco AI Endpoint Analytics uses the Application Hosting capability that is available on the switches to enable scans for open ports and weak credentials.

Enable and monitor sensor scans

Before you begin

- Connection to Cisco ISE Release 3.1 or later releases, if you want to enforce endpoint policies based on the scan results.
- Connection to Cisco Catalyst 9300 or 9400 Series devices.
- Ensure that the switches are upgraded to Cisco IOS XE Release 17.7.1 or later releases.

Procedure

Step 1 Log in to your Catalyst Center.

Step 2 From the main menu, choose **Policy** > **AI Endpoint Analytics**.

Step 3 In the **Overview** window that displays, click **Configurations**.

Step 4 From the left pane, choose **Trust Analytics**.

Step 5 In the **Security Sensor** area, the prerequisites for using the sensor scans feature to identify open ports and weak endpoint credentials display. Click the corresponding links in this area to carry out these tasks:

a. Verify the supported Catalyst Center and Cisco IOS-XE releases from the release notes for Cisco Catalyst 9000 Series devices. Download the security sensor container from software.cisco.com for the relevant Cisco Catalyst 9000 Series device. A .tar file downloads to your system.

b. Install App Hosting in your Catalyst Center. See Application hosting, on page 1134 for instructions.

c. Upload the .tar file in your Catalyst Center **App Hosting** window. The link to the **App Hosting** window displays in the **Security Sensor** area.

d. Install and enable the .tar file in each Cisco Catalyst 9000 Series device that you want to enable sensor scans on.

In your Catalyst Center **App Hosting** window, check that the **App Hosting Status** is active for least one of the Cisco Catalyst 9000 Series devices on which you enabled the .tar file.

Step 6 After the active probes container is installed and enabled as explained in the previous step, in the **Security Sensor** area, you can configure Trust Score settings in Cisco AI Endpoint Analytics to scan for open ports and weak credentials on endpoints that are connected to Cisco ISE and the Cisco Catalyst devices on which the active probes application is enabled.

- Click the **Open Port Scan** toggle button to enable Cisco AI Endpoint Analytics to proactively run port scans to detect and close possible vulnerabilities on defined endpoints on the network.
- Click the **Credential Vulnerability Scan** toggle button to enable Cisco AI Endpoint Analytics to proactively detect when endpoints on your network are using weak credentials in order to prevent malicious activity.

Step 7 (Optional) If you choose to enable scanning for open ports, you can define the scan by clicking **Scan Configuration** in the **Open Port Scan** area.

a) In the **Scan Configuration** window, in the **Defined Scans** tab, click the **Define Scan** button.
b) A dialog box displays that allows you to define the scope of a port scan:
   - To scan each endpoint at the time of endpoint enrollment, choose the **On enrollment, scan all endpoints** radio button.
   - To define the scope of the open port scan by subnet, profiling attributes, and more, choose the **Create a Custom Scan** radio button.

   In both types of port scan, you define a list of unauthorized ports to specify the ports that must always be closed. This list allows Cisco AI Endpoint Analytics to recognize anomalous port activity on an endpoint and assign it a low trust score. For both port scan types, the minimum frequency of scan that you can configure is 12 hours.
c) In the **Scan Configuration** window, in the **Open Ports List** tab, specify the type and range of ports, or individual ports, that must be scanned.
d) In the **Scan Configuration** window, in the **Unauthorized Ports** tab, define by port number and port type, the ports that are unauthorized in your network. If Cisco AI Endpoint Analytics detects these ports as active, the endpoint is given a low trust score for the anomaly of an active unauthorized port.

Step 8 (Optional) If you choose to enable the detection of weak credentials, you can define the scan by clicking **Scan Configuration** in the **Credential Vulnerability Scan** area. SSH and TELNET protocols are supported by this feature.

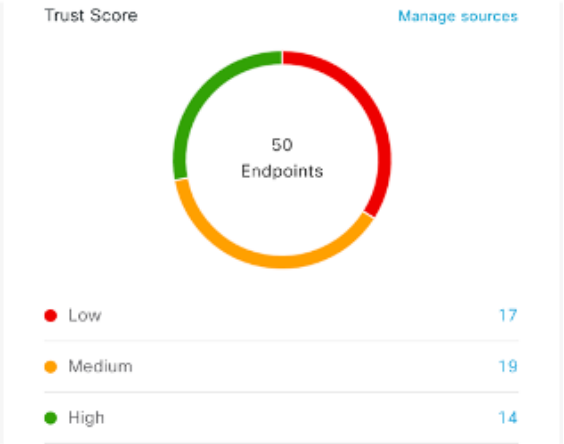
a) In the **Credential Vulnerability Scan** window, in the **Scan** tab, define a list of credentials that you want to identify as weak credentials. Define lists of usernames and passwords that are considered vulnerable according to your enterprise requirements.
b) In the **Credentials** tab, a default list of more than 3500 weak credentials is available by default. You can use this default list to create a credential vulnerability scan. To add a new list of vulnerable credentials, click **Create New List**.

The minimum frequency of credential vulnerability scan that you can configure is 12 hours.

Step 9 For the scans that you enable in the **Security Sensor**, the relevant endpoints are scanned and if anomalies are detected in open ports or credential checks, the Trust Score for these endpoints is adjusted accordingly. In the **Endpoint Inventory** tab, where applicable, the **Trust Score** tab for an endpoint displays the list of unauthorized ports that are open on the endpoint, or weak usernames, or both.

View and manage Trust Scores for endpoints

Figure 35: Trust Score dashlet in Cisco AI Endpoint Analytics Overview tab



After Catalyst Center is upgraded and necessary Trust Score sources are enabled, the Cisco AI Endpoint Analytics **Overview** tab (main menu > **Policy** > **AI Endpoint Analytics**) displays the **Trust Scores** dashlet. This dashlet contains this information:

- The total number of endpoints that have been assigned a Trust Score.
- A donut chart and a list of the number of endpoints with low, medium, and high trust scores.

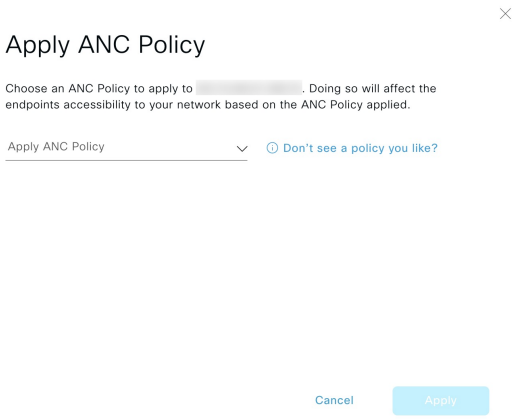
To view the details of endpoints in a trust score category, click its endpoint count in the **Trust Scores** dashlet. The **Trust Score** view of the **Endpoint Inventory** tab displays with the appropriate filters applied.

You can view endpoints with Trust Scores in two ways:

- In the **Trust Score** tab, choose the **Endpoints** tab to see all the endpoints with Trust Scores assigned.
- In the **Endpoint Inventory** tab, click **View endpoints in Trust Score View** from the caution message that is displayed, to see endpoints with Low and Medium scores.

You can do these actions on endpoints with Trust Scores:

- **Apply an ANC Policy**



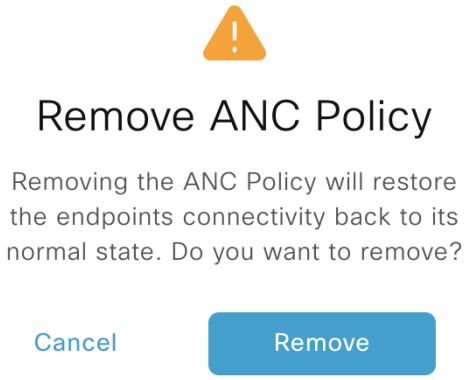
Click the **Apply ANC Policy** button to choose an ANC policy to be applied to an endpoint. The endpoint's access to the network is modified accordingly. ANC policies are imported from Cisco ISE and displayed in the drop-down list in the pop-up window displayed.

- **Replace an ANC Policy**



Click **Change ANC Policy** button to replace an existing ANC policy of an endpoint with another ANC policy. From the pop-up window displayed, choose the new policy to be applied from the **Change ANC Policy** drop-down list.

- **Remove an ANC Policy**



Click the **Remove ANC Policy** button to remove an applied ANC policy from an endpoint. In the pop-up window displayed, click **Remove**. This removes the remediation policy that was applied to the endpoint, and allows the endpoint to connect to the network normally.

- **Reset Trust Score**

Figure 36: Reset Trust Score for an endpoint without an ANC Policy

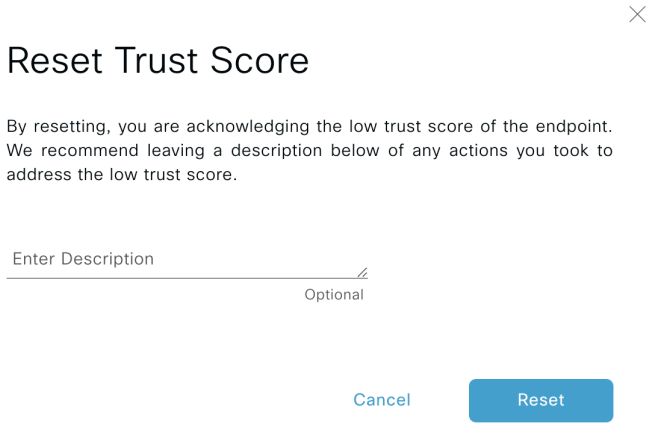
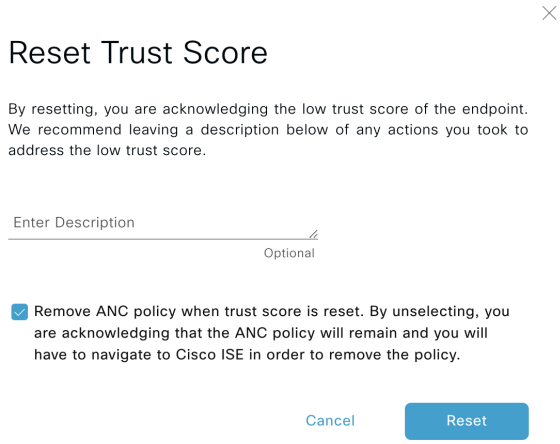


Figure 37: Reset Trust Score for an endpoint with an ANC Policy



Click **Reset Trust Score** button to remove an endpoint from the Trust Score inventory. In the pop-up window displayed, click **Reset**.

If you choose this option for an endpoint after applying an ANC policy, you will not see this endpoint in the Trust Score inventory again. In this case, to modify the ANC policy for such an endpoint, you must remove the policy from Cisco ISE instead.

If you reset the score for an endpoint without applying an ANC policy, you may see the endpoint in the Trust Score inventory again with the next automatic refresh of Trust Score data.

The buttons for each of the actions displays in two locations in the **Endpoint Inventory** tab. The actions can be done on a single endpoint, or on multiple endpoints.

- **Manage Trust Score for a single endpoint**

Figure 38: Trust Score options for an endpoint without an ANC Policy

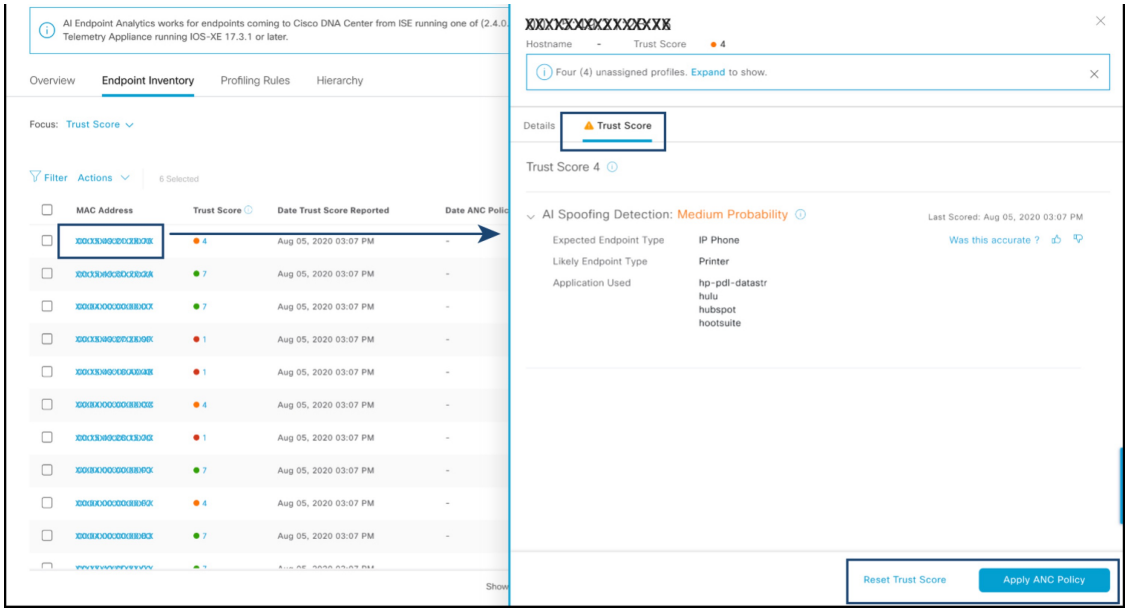
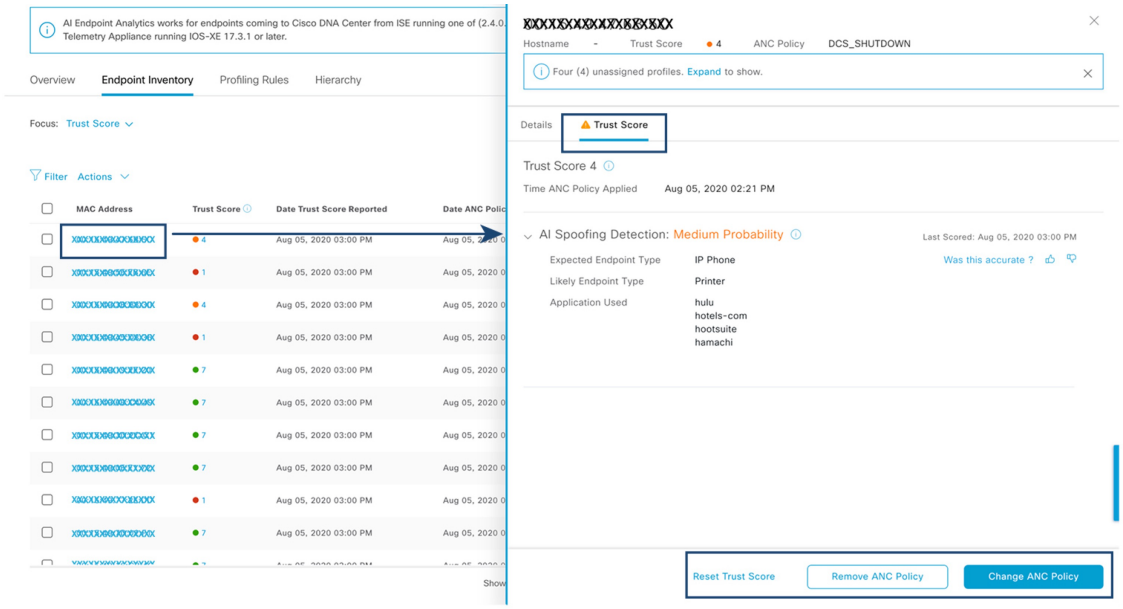


Figure 39: Trust Score options for an endpoint with an ANC Policy



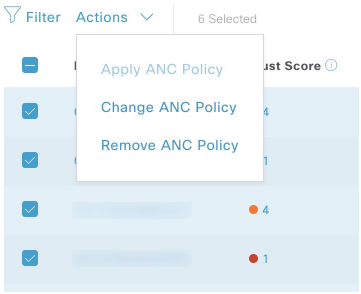
From the list of endpoints with a Trust Score, click the MAC Address of the endpoint you want to manage. In the endpoints details pane that displays, click the **Trust Score** tab.

Here, **Expected Endpoint Type** value is displays. The **Applications Used** field lists the applications that are used by the endpoint.

This pane includes buttons to start the workflows of accepting and removing ANC policies, and to reset the Trust Score. Click the button for the intended task.

Alternatively, you can check the check box for an individual endpoint on the **Endpoint Inventory** window, click **Actions**, and choose the required option from the drop-down list.

- **Manage Trust Score for multiple endpoints**



In the **Endpoint Inventory** tab, check the check boxes for all the endpoints you must do a specific action on. Click **Actions** and choose the required action from the drop-down list.

Control endpoint spoofing

Concurrent MAC address detection means that two endpoints with the same MAC address are detected accessing the network and generating traffic. It then becomes imperative to distinguish between the real endpoint and the spoofed endpoint and take the necessary remediation action for the spoofed endpoint.

The Control Endpoint Spoofing feature provides granular policy control by providing network information other than just the MAC address of an endpoint. Network information includes site information, network device IP address, network device port, first authorized timestamp, last authorized timestamp, and the duration for which the endpoint has been available in the network. You can choose to distinguish the entries by the MAC address as done traditionally, or by using both the MAC address and the network information provided. If you choose to distinguish by MAC address and connectivity (network information), a selection is made automatically to detect the spoofed endpoint. You can either go with the automatic selection or choose the one you feel is the spoofed endpoint, and apply the appropriate remediation action for that endpoint. The remediation actions available are the Adaptive Network Control (ANC) policies configured in Cisco ISE.

Because this is the granular way of applying the policy, you won't see a listing for this policy in **Operations** > **Adaptive Network Control** > **Endpoint Assignment**.

For endpoints without concurrent MAC address detection and only NAT mode detection, an ANC policy is applied as described in View and manage Trust Scores for endpoints, on page 1312. In such a scenario, the endpoint gets listed under **Endpoint Assignment** in Cisco ISE.

For endpoints with both concurrent MAC addresses and NAT mode detection, the precedence is given to granular policy control. So, when you click **Apply ANC Policy**, you get the new **Apply ANC Policy** window with two options, to distinguish the entries.

You can also choose to change the ANC policy for an endpoint at any point of time. While changing the ANC policy, you have an option to choose more than one entry for which the ANC policy can be applied.

Note If you chose **Shutdown** as the remediation action, and you want to change the action, the endpoint won't be brought back automatically after changing the action. You must manually turn on the interface in the switch to which the endpoint is connected.

An ANC policy can also be removed at any point of time.

Before you begin

The dynamic author must be configured in the network devices. We recommend that you provision the network devices with the AAA configuration from Catalyst Center.

Procedure

Step 1 From the Catalyst Center GUI, choose **Policy** > **AI Endpoint Analytics** > **Endpoint Inventory** > **View endpoints in trust score view**.

Step 2 Click the endpoint that you want to check and apply the ANC policy to.

Step 3 Choose **Trust Score** > **Concurrent MAC Address**.

Step 4 Click **Apply ANC Policy**.

Step 5 In the **Apply ANC Policy** window, choose **Based on MAC address** or **Based on MAC address and connectivity**.

Step 6 Choose the appropriate remediation action from the **Apply ANC Policy** drop-down list.

Step 7 Click **Apply ANC Policy**.

After completing this task, when you return to the **Trust Score** view for that endpoint, you can see the ANC policy name and the network device IP address to which the policy was applied, along with the time at which the ANC policy was applied.

To verify the configuration, in the Cisco ISE GUI, choose **Operation** > **RADIUS** > **Live logs**. You can filter the **Identity** column by endpoint MAC address.

An entry for the CoA action that was initiated from Cisco ISE for this endpoint is listed. If you check the details, the **CoA Reason** shows the ANC policy that was applied by you for the endpoint.

Profiling rules

Profiling rules in Cisco AI Endpoint Analytics enable you to group endpoints with a combination of common attributes. These attributes allow endpoint identification by Endpoint Type, OS Type, Hardware model, and Hardware Manufacturer. The profiling rules help you administer and manage many endpoints with ease.

Cisco AI Endpoints Analytics receives profiling data from network devices through DPI, media protocols, medical industry protocols, and more. Profiling data from Cisco ISE is communicated through pxGrid. These profiling attributes are then available in the device dictionary for authoring profile rules.

You can view the profiling rules in the **Profiling Rules** tab of Cisco AI Endpoints Analytics. In the table that displays under this tab, click a **Rule Name** entry to view the assigned profiles and attributes used.

The profiling rules that are used to profile the endpoints in Cisco AI Endpoint Analytics are:

- System Rules
- Custom Rules
- Cisco AI Rules

Rule prioritization

The profiling rules in Cisco AI Endpoint Analytics have an order of priority. Profiling rule execution follows this rule priority to profile endpoints with high fidelity.

As user inputs are primary in Cisco AI Endpoint Analytics, the priority of the profiling rules include:

- Administrator-created static profiles, for example, profiles added using the **Register Endpoints** option.
- Administrator-created custom rules.
- Cisco-provided system rules that are available by default.
- Auto-generated rules through the machine learning-enabled Smart Grouping workflow.

To view the set rule priority, click **Rule Prioritization** in the **Profiling Rules** window.

A registered endpoint can be profiled by multiple Cisco AI Endpoint Analytics rules for different profiling labels. This table shows the design of profiling rules for two endpoints.

Endpoint 1	Endpoint 2
Hardware Model profiled by System Rule	Hardware Model profiled by System Rule
OS Type profiled by Cisco AI Rule	Hardware Model profiled by Custom Rule
Hardware Manufacturer profiled by Custom Rule	Hardware Model profiled by Cisco AI Rule

For Endpoint 2, rule priority results in the precedence of the custom rule over the others. The Hardware Model label for Endpoint 2 is profiled by the custom rule.

For Endpoint 1, different rules define different profile labels, and each label is profiled accordingly.

Filter profiling rules

Procedure

Step 1 In the **Profiling Rules** window, click **Filter**.

Step 2 Enter a name in the **Rule Name** field.

Step 3 Select values for endpoint attributes from the corresponding drop-down lists, to filter for a set of endpoints.

Step 4 Click **Apply**.

View updated profiling rules

Procedure

Step 1 Go to the **Endpoint Inventory** window.

Step 2 Click the check box adjacent to the MAC address of the endpoint to view the profiling details of the endpoint.

Step 3 Click the information icon next to profile labels, and click the rule name to view the assigned profile and attributes details.

System rules

Cisco AI Endpoint Analytics provides predefined rules called System rules for profiling endpoints. When Cisco AI Endpoint Analytics deploys, it provides day-zero visibility into endpoints without any need to configure specific rules.

Newly onboarded endpoints are profiled using system rules by default.

Network devices are managed in Catalyst Center in the **Provision** > **Network Devices** > **Inventory** window.

These network devices are profiled by the system rules and are not visible in the Cisco AI Endpoint Analytics **Endpoint Inventory** window. However, you can view the endpoints profiled by custom rules because the custom rules are created with the network device as **Device Type**.

Automatic system rule updates for endpoint profiling

The system rules that are used for endpoint profiling in Cisco AI Endpoint Analytics are regularly updated to enhance profiling accuracy. Schedule automatic updates to receive updates in endpoint profiling system rules from Cisco. Your Catalyst Center receives updates at the configured time, and the changes are applied in Cisco AI Endpoint Analytics. In the **Profiling Rules** window (**Policy** > **AI Endpoint Analytics** > **Profiling Rules**), review the details of the changes in endpoint profiles, and accept or decline the system rule update.

If an endpoint's hardware model value changes due to an accepted system rule update, when you view the endpoint's details in the **Endpoint Inventory** tab, the **Hardware Model** field contains the name of the system rule update.

Before you begin

Configure and enable NBAR Cloud. See Configure CBAR cloud, on page 1117.

To check the status of NBAR Cloud, choose **Policy** > **AI Endpoint Analytics** > **Overview**, and click **Configuration**.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Profile Rule Settings**.

The **Enabled** toggle button in the **Schedule Automatic Updates** area is set to active by default.

Step 2 Click the buttons for the days of the week on which you want to schedule updates. You can select multiple days. Then, use the **Time Slot** text fields to select the time for the update. It takes 30 minutes for the updates to be received by Catalyst Center. The second time slot area is not editable and displays the time when the scheduled update is expected to complete.

Step 3 When your Catalyst Center receives a system rule update, a notification is displayed in the **Profiling Rules** window (**Policy** > **AI Endpoint Analytics** > **Profiling Rules**). These notification display when you click **Expand** in the dialog box:

You are updated to the latest version *Name of Latest Version* and a recent Cisco profiling rule has changed the profiles of some endpoints.

Click **Review Update**.

Step 4 The **Endpoint Profile Update Review** dialog box displays. The dialog box contains information on the current stable update applied, the latest update received, and more. It also contains these sections that you can click to view the related endpoint profile updates:

a. **Major Updates**: Lists the endpoints whose profiles have had major changes, such as a Windows endpoint that is now recorded as a Linux endpoint.

b. **Minor Updates**: Lists the endpoints whose profiles have had minor changes, such as an updated version of Windows OS.

c. **Newly Profiled**: Lists the endpoints that were unprofiled previously and have now been assigned profile information.

Step 5 After you review the endpoint profile changes, to accept the profile update, click **Mark As Approved Version** in the **Endpoint Profile Update Review** dialog box. If you do not agree with the endpoint profile changes, click **Rollback**.

When you select rollback, you must select if you want to roll back to the last running version, or the last approved version, by clicking the corresponding option.

You can also perform the accept and rollback actions from the **AI Endpoint Analytics** > **Overview** > **Configuration** window.

Step 6 Click **X** to close the dialog box.

Custom rules

In addition to the system rules, you can also create custom rules for profiling endpoints using a combination of endpoint attributes. Custom rules precede all the other endpoint profiling rules in Cisco AI Endpoint Analytics.

Logic and conditions for profiling rules

You can create custom profiling rules in the **Endpoint Inventory** window. To create a custom profiling rule, you must create a logical condition based on endpoint attributes and values. These attributes are collected from network probe data and are different from the classification attributes available in the **Attribute Glossary** window.

A value is a user input that uniquely identifies the group of endpoints. The attributes and values create a regular expression with the help of the operators in this table.

Operators	Description
Contains	Attribute has the selected value.
Equals	Attribute is strictly mapped to the selected value.
Matches	Attribute should match the regular expression pattern of the selected value.
Starts With	Attribute should start with the selected value.

Note Contains, Equals, and Starts With are case-sensitive operators. For case-insensitive values, use the Matches operator.

These conditions can be further combined with the help of logic (**AND** and **OR**) to create a nested rule.

Create and Edit a Logical Condition

Follow the below instruction to create a logical condition.

Procedure

Step 1 In the **Choose Attribute Conditions** window, check the check box adjacent to the **Attribute** that you want to update.

Step 2 Choose a option from the **Operator** drop-down lists.

Step 3 Enter the value in the **Value** field.

Step 4 Click **Next**.

Step 5 In the **Add Logic to Conditions** window that is displayed, drag and drop the **AND** logic or the **OR** logic between the conditions in order to create a logical sequence of conditions for a custom rule.

Note You can also add or edit an attribute condition in the **Add Logical Conditions** window using the vertical ellipsis next to a condition.

Step 6 Click **Next**.

Create a custom rule

Procedure

Step 1 In the **Endpoint Inventory** window, check the check box adjacent to the MAC address of the endpoints that you want to profile.

Step 2 Click **Actions** and choose **Profile with Custom Rules**.

Step 3 In the **Name Rule and Type** window that displays, in the **Rule Name** field, enter a name for the rule, and from the **Profile Label** drop-down list, choose a label.

Depending on what you choose from the **Profile Label** drop-down list, a corresponding field, whose name is dynamically updated, is displayed. For example, if you choose **Endpoint Type**, the **Endpoint Type** field appears.

Step 4 Enter a value in the new field that displays. As you start entering information, matching options display. If an option matches your requirements, select the same. Otherwise, enter the complete type name.

Step 5 Click **Next**.

Step 6 In the **Choose Attribute Conditions** window that displays, create a logical condition.

For more information, see Logical Conditions.

Step 7 In the **Review Rule** window, review the list of endpoints that are going to be profiled with this custom rule.

Step 8 Click **Next**.

Step 9 Click **Profile**.

Edit a custom rule

Procedure

Step 1 In the **Profiling Rules** window, check the check box adjacent to the admin rule you want to edit.

Step 2 Click **Actions** and select **Edit**.

Step 3 In the **Edit** window that displays, in the **Rule Name** field, enter a name for the rule, and select or enter the profile details based on the **Profile Label** selected during the rule creation.

Step 4 In the **Logic and Conditions** section, click on the vertical ellipsis and select **Edit** to update the logic and conditions for profiling rules. For more information, see **Logical Conditions**.

Step 5 Click **Next**.

Step 6 Click **Apply**.
After the existing rule updates with new profiling details, the endpoints profiled with this rule update with new profiling details.

Delete a custom rule

Procedure

Step 1 In the **Profiling Rules** window, check the check box next to the rule that you want to delete.

Step 2 Click **Actions** and choose **Delete**.

This message is displays:

```
Do you really want to delete the selected Rule(s)?
```

Step 3 Click **Yes** to permanently delete the rule from Cisco AI Endpoint Analytics.
After the custom rule is deleted, the endpoints profiled with this rule are updated with system rules.

Export and import custom profiling rules across deployments using APIs

Catalyst Center contains Cisco AI Endpoint Analytics APIs through which you can import, export, edit, and delete custom profiling rules.

To enable the Cisco AI Endpoint Analytics API bundle:

1. From the main menu, choose **Platform** > **Manage** > **Bundles**.
2. Find the bundle named **AI Endpoint Analytics** and click **Enable**.
3. The value in the **Status** column changes from **Disabled** to **Active**, and the list of APIs display. You can also view the expected request and response payloads for each API.
4. After you enable the API bundle, the Cisco AI Endpoint Analytics APIs are added to the Catalyst Center Developer Toolkit. You can then access the APIs from the **Developer Toolkit** window (**Platform** > **Developer Toolkit**).

From both the **Bundles** and **Developer Toolkit** windows, you can:

- Generate code preview to view the API code that you can use in a different tool to run the API.
- Click **Try It** to run the API from the Catalyst Center GUI. You will receive a JSON response that you can copy and paste into a text editor of your choice to continue working with.

Cisco AI rules for smart grouping

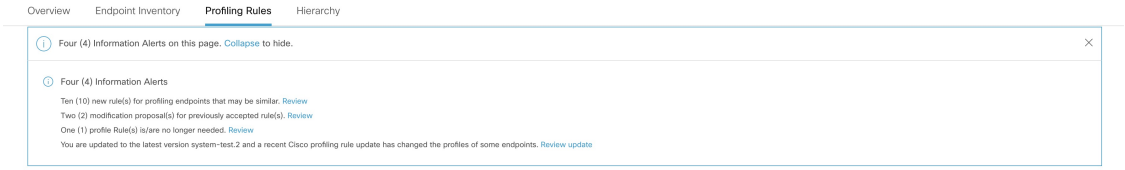
The Cisco AI Endpoint Analytics' AI algorithm analyzes data about endpoint profiling labels and groups across deployments and provides you with smart profiling rules suggestions.

The **AI Proposal** dashlet in the Cisco AI Endpoint Analytics **Overview** tab displays these rule suggestions based on the learnings from endpoint clusters:

- New profiling rules for unprofiled or unlabeled endpoints in your network. For more information, see New profiling suggestions for similar endpoints in your network, on page 1324

You can also initiate the workflows to review and apply proposals for changes to endpoint profiling rules from the **Profiling Rules** tab of Cisco AI Endpoint Analytics. The **Profiling Rules** displays a dialog box with information alerts. In the information alert dialog box, click **Expand** to view the available proposals for changes to endpoint profiling rules. Click **Review** next to the information alert that you want to examine to initiate the corresponding workflow.

Figure 40: Information alerts in the Profiling Rules tab



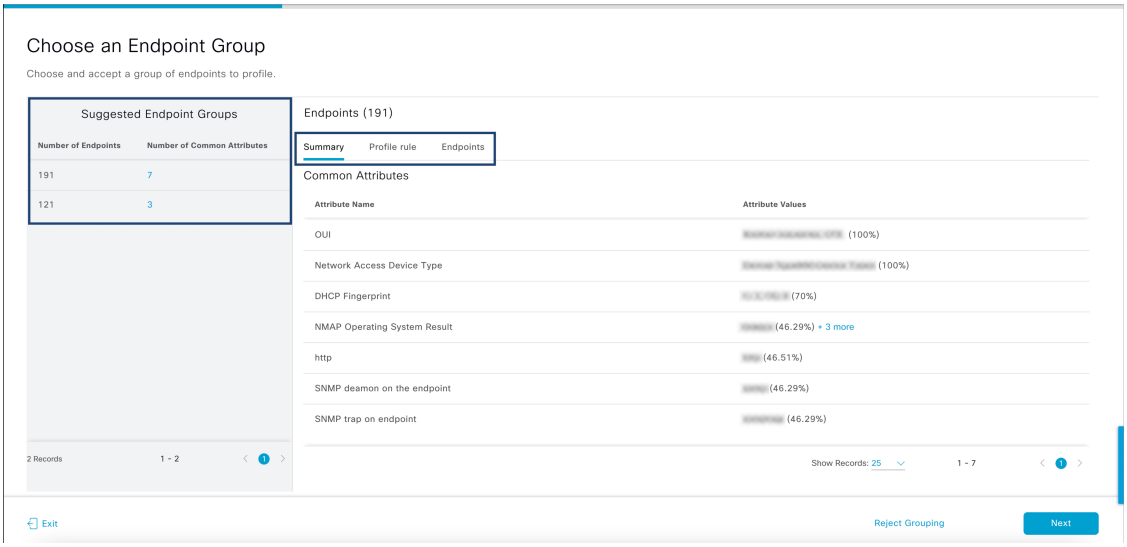
New profiling suggestions for similar endpoints in your network

Procedure

Step 1 In the **AI Proposals** dashlet, click the **Review** button next to **New rule(s) for profiling endpoints that many be similar**. The **Smart Group Profile** workflow is launched.

Step 2 The **Choose an Endpoint Group** window that displays contains a list of new profiling rules suggestions in the left pane. Click an entry in the list to view the details of the profiling rule in the right pane.

Figure 41: Choose an Endpoint Group window of the Smart Group Profile workflow

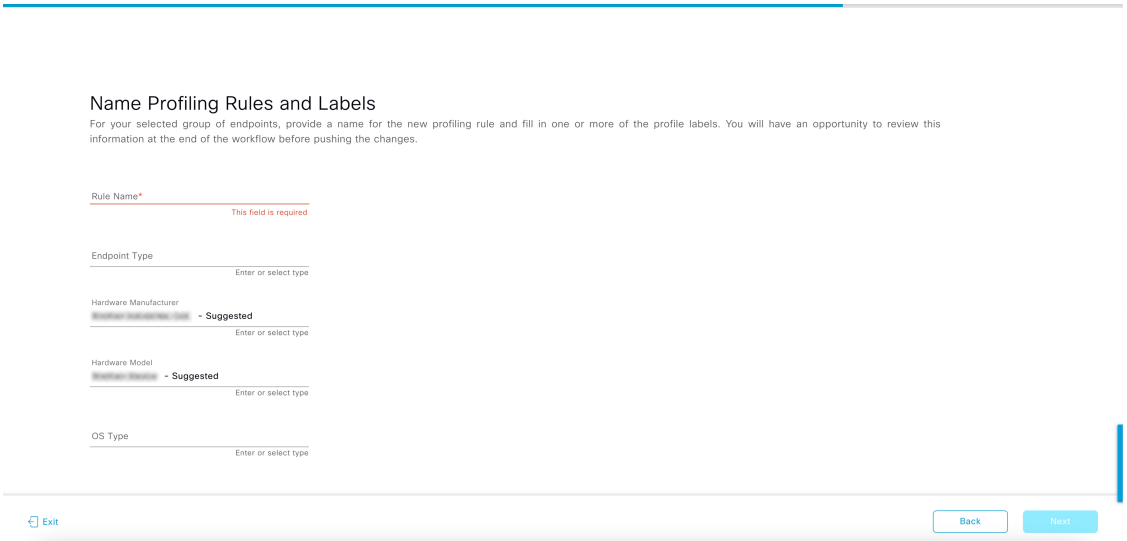


The right pane contains the **Summary**, **Profile Rule**, and **Endpoints** tabs that provide a quick view of the details of the profiling rule that is suggested.

Step 3 Click **Next** to create the suggested profiling rule.

Step 4 In the **Name Profiling Rules and Labels** window that is displayed, in the **Rule Name** field, enter a name for the rule.

Figure 42: Name Profiling Rules and Labels window of the Smart Group Profile workflow



Step 5 In one or more of these fields, enter the required values:

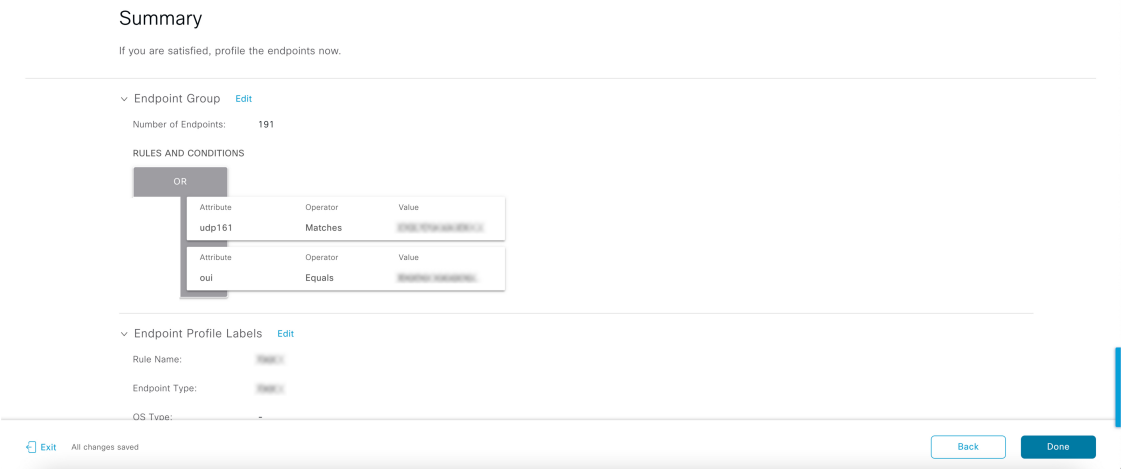
- **Endpoint Type**
- **Hardware Manufacturer**
- **Hardware Model**
- **OS Type**

If the AI algorithm identifies a profiling label for the endpoints, the label displays as a suggestion in the corresponding field. You can choose to proceed with the suggested label or select a different label.

Step 6 Click **Next** to continue.

Step 7 In the **Summary** window, review the details of profiling rule. To make any changes, click **Edit**.

Figure 43: Summary window of the Smart Group Profile workflow



Step 8 To create the profiling rule, click **Done**.

Import profiling rules

You can migrate your custom profiling rules and Cisco AI rules by importing the .json files.

Procedure

Step 1 In the **Profiling Rule** window, click **Actions**

Step 2 Choose **Import Profiling Rules**.

Step 3 Click **Choose a file** and browse to the .json file in your system.

Step 4 Click **OK**.

Export profiling rules

You can export and back up custom rules and Cisco AI profiling rules from Cisco AI Endpoint Analytics. The **Export Profiling Rules** option exports all the available custom rules and Cisco AI profiling rules. You cannot selectively export rules.

Procedure

Step 1 In the **Profiling Rules** window, click **Actions**.

Step 2 Choose **Export Profiling Rules**.

Step 3 Click **Yes** to export all the custom and ML profiling rules. Click **No** to exit.

Note You can import the same file again into Cisco AI Endpoint Analytics.

Hierarchy

Cisco AI Endpoint Analytics hierarchy helps you create logical groupings of endpoints, based on the endpoint types. Creating categories and subcategories for the endpoints focuses on endpoint visibility and simplifies the authorization process.

You can create categories from the **All Endpoints** default parent category. The category details such as total number of endpoints, endpoint types, and subcategories are listed within individual boxes in the **Hierarchy** window.

You can create, edit, and delete the categories to reorder the hierarchy.

Create category and subcategory

Procedure

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the parent category.

Step 2 Click **Create Category**.

Step 3 Enter a category name.

Step 4 Click **Enter**.

What to do next

After you create a category, you can drag and drop endpoint types from the **Endpoint Type** window, or edit the category to add endpoints to it.

Edit a category or subcategory

Procedure

Step 1 In the **Hierarchy** window, click on the horizontal ellipsis of the category.
Step 2 Click **Edit**.
Step 3 In the **Edit** window that displays, enter the **Category Name**.
Step 4 Enter the **Parent Category** from the drop-down menu, if you want to reassign the category.
Step 5 Click the **Endpoint Type** tab.
Step 6 Click **Actions** and select **Add Endpoint Type**.
Step 7 Choose the endpoint type from the **Search Dropdown** list.
Step 8 Click **Save**.

What to do next

In the Endpoint Type window, you can filter the endpoint types as **All**, **Available**, and **Assigned**.

Delete endpoint types from category

Procedure

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category that you want to delete.
Step 2 Click **Edit**.
Step 3 In the **Edit** window, click the **Endpoint Type** tab.
Step 4 Check the check box adjacent to the endpoint type that you want to delete.
Step 5 Click **Actions** and choose **Remove From Category**.

This message displays:

```
Are you sure you want to delete this category?
```

Step 6 Click **Yes** to delete the endpoint from the category. Click **No** to exit.

Reassign endpoint types from category

Procedure

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category.
Step 2 Click **Edit**.

Step 3 In the **Edit** window, click the **Endpoint Type** tab.

Step 4 Check the check box adjacent to the endpoint type that you want to reassign.

Step 5 Click **Actions** and choose **Re-assign to existing category** or **Re-assign to a new category**.

Option	Steps
Re-assign to existing category	**a.** In the **Reassign** window, choose an existing category from the **Category** drop-down list. **b.** Click **Save**.
Re-assign to a new category	**a.** In the **Reassign** window, choose **New Category** from the **Category** drop-down list. **b.** Choose a parent category from the **Parent Category** drop-down list. **c.** Enter the category name in the **New Category** field. **d.** Click **Save**.

Delete a category

Before you begin

Before you delete a parent category, check its subcategories. You can reassign the subcategories to another existing category or to a new category. Otherwise, all the subcategories are deleted along with the parent category. You can also reassign the subcategories while you are deleting a category.

Procedure

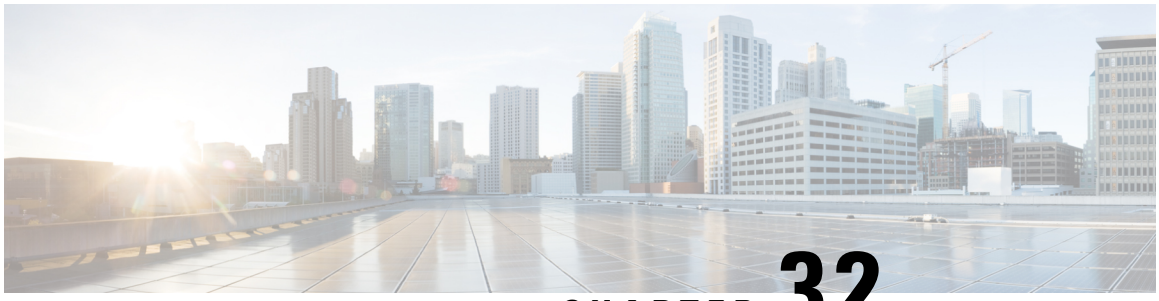
Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category.

Step 2 Click **Delete**.

If you are deleting a category that has subcategories assigned to it, the **Reassign Relationships** dialog box displays. Choose one of these options:

Option	Condition	Steps
Reassign to an existing category	Reassign the subcategories to an existing category.	**a.** Select a category from the **Category** drop-down list. **b.** Click **Reassign**. The parent category is deleted and its subcategories will be reassigned to the selected category.

Option	Condition	Steps
Reassign to a new category	Reassign the subcategories to an existing category.	**a.** Select a category from the **Parent Category** drop-down list. **b.** Enter the category name in the **New Category** field. **c.** Click **Reassign**. The parent category is deleted and its subcategories are reassigned to the new category.
Remove from category	Delete the subcategories along with the parent category.	Click **Reassign**. The parent category and its subcategories are deleted.



CHAPTER 32

Troubleshoot Network Devices Using Network Reasoner

- Network Reasoner overview, on page 1331
- Validate Cisco SD-Access migration using the MRE workflow, on page 1331
- Troubleshoot high CPU use, on page 1333
- Troubleshoot a power supply failure, on page 1335
- Troubleshoot a downed interface, on page 1336
- Troubleshoot network connectivity, on page 1337
- Troubleshoot IP connectivity of a device, on page 1338
- Troubleshoot wireless clients using the MRE workflow, on page 1339
- Troubleshoot wireless APs using the MRE workflow, on page 1340
- Troubleshoot unmonitored devices using the MRE workflow, on page 1341
- Troubleshoot HA on Cisco Wireless Controller using the MRE workflow, on page 1341

Network Reasoner overview

The Network Reasoner tool allows you to troubleshoot various issues on your network quickly. From the main menu, choose **Tools** > **Network Reasoner** to launch the Network Reasoner dashboard. The Network Reasoner dashboard hosts separate workflows that you can use to proactively troubleshoot network issues. The dashboard provides a brief description of the workflows, the number of affected devices in the last 24 hours, and the impact of running a workflow on a network.

Note You must install the Machine Reasoning package to view the Network Reasoner feature under the **Tools** menu. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Validate Cisco SD-Access migration using the MRE workflow

These Machine Reasoning Engine (MRE) workflows assist in planning your migration to Cisco SD-Access:

- SDA Hardware Readiness Check
- SDA Software Readiness Check

- Redundant Link Check
- L3 Access Check
- MTU Link Check
- SDA Health Check
- SDA Scale Limits Check

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 In the **Network Reasoner** dashboard, click the workflows as required:

Workflow	Description	Action
SDA Hardware Readiness Check	Checks whether the hardware is ready for Cisco SD-Access migration.	**a.** Click **SDA Hardware Readiness Check**. **b.** Click **Run Machine Reasoning**.
SDA Software Readiness Check	Checks whether the software is ready for Cisco SD-Access migration.	**a.** Click **SDA Software Readiness Check**. **b.** Click **Run Machine Reasoning**.
Redundant Link Check	Checks whether any redundant uplinks are present in your device and if there are ways to increase availability by configuring redundant uplinks on the access switches.	**a.** Click **Redundant Link Check**. **b.** Select an appropriate device. **c.** Click **Troubleshoot**.
L3 Access Check	Checks whether your network has access switches that are running Layer 3 routing protocols to move to Cisco SD-Access with minimal design changes.	**a.** Click **L3 Access Check**. **b.** Select an appropriate device. **c.** Click **Troubleshoot**.
MTU Link Check	Checks whether the links between the main network devices and the access, core, and other switches are configured with the correct MTU.	**a.** Click **MTU Link Check**. **b.** Select an appropriate device. **c.** Click **Troubleshoot**.
SDA Health Check: Fabric Count	Checks the health of the Catalyst Center cluster to determine whether it is reaching any scale limit thresholds due to managing fabrics.	**a.** Click **Fabric Count**. **b.** Click **Run Machine Reasoning**.

Workflow	Description	Action
SDA Health Check: Fabric Data Collection	Collects show command outputs from network devices to troubleshoot issues in a fabric network.	**a.** Click **Fabric Data Collection**. **b.** Choose the devices and click **Troubleshoot**. **c.** After Machine Reasoning is completed, click **View Details.** **d.** In the **Conclusions** tab, click the link to download the output file. The output file is a bundle of text files containing all executed commands on the selected devices.
SDA Health Check: SDA Scale Limits Check	Checks whether the number of client endpoints, network devices, and configured fabrics in Catalyst Center are within the published SDA limits.	**a.** Click **SDA Scale Limits Check**. **b.** Click **Run Machine Reasoning**.
SDA Health Check: Client Count	Checks the health of the Catalyst Center cluster to determine whether it is reaching any scale limit thresholds due to managing clients.	**a.** Click **Client Count**. **b.** Click **Run Machine Reasoning**.
SDA Health Check: Device Count	Checks the health of the Catalyst Center cluster to determine whether it is reaching any scale limit thresholds due to managing network devices.	**a.** Click **Device Count**. **b.** Click **Run Machine Reasoning**.
SDA Health Check: LISP PubSub Session Check	Checks the LISP PubSub health on the fabric border device. If a PubSub session is down, troubleshoot to find the root cause.	**a.** Click **LISP PubSub Session Check**. **b.** Choose the devices and click **Troubleshoot**. **c.** After Machine Reasoning is completed, click **View Details**.
SDA Health Check: LISP Session Check	Checks the status of all LISP sessions on the chosen device. If a session is down, troubleshoot to find the root cause	**a.** Click **LISP Session Check**. **b.** Choose the devices and click **Troubleshoot**. **c.** After Machine Reasoning is completed, click **View Details**.

Troubleshoot high CPU use

CPU use troubleshooting support is available only for these network devices with software version 16.9.3 and later:

- Cisco Catalyst 9400 Series Switches

- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the Cisco Catalyst Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see "Configure Role-Based Access Control" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **CPU Utilization** tab.

The **CPU Utilization** window displays the filtered list of devices with high CPU use in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

Step 5 In the **Reasoner Input** window, enter the **CPU Utilization Threshold** percentage that you want to check against.

Step 6 Click **Run Machine Reasoning**.

Note These processes, if observed, are considered for detailed analysis:

- **MATM Process Group**: MATM RP Shim, NGWC Learning, and VMATM Callback
- **IOSXE Process Group**: IP Input, ARP Input, IOSXE-RP Punt Se, SISF Main Thread, DAI Packet, and ARP Snoop

In the **CPU Utilization** window, you can see the **Root Cause Analysis** of the high CPU use for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 7 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 8 Click the **Conclusion** tab to see the processes that consume more CPU and the use percentage.

Step 9 Click **View Relevant Activities** for each process to view the **Activity Details** in the right pane.

Step 10 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The Machine Reasoning Engine (MRE) implements a system-end algorithm that detects and ends network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot a power supply failure

Power supply troubleshooting workflow support is available only for these network devices with software version 16.6.1 and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the Cisco Catalyst Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see "Configure Role-Based Access Control" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **Power Supply** tab.

The **Power Supply** window displays the filtered list of devices with power supply failures in the past 24 hours.

Click **All** to see the list of all devices in the inventory. You can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and filter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

In the **Power Supply** window, you can see the **Root Cause Analysis** of the power supply failure for the chosen device.

The **Reasoning Activity** tab displays the various parameters that are checked as part of the troubleshooting process.

Step 5 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 6 Click the **Conclusion** tab to see the **Stack Identifier**, **Product ID**, **Serial Number**, and **Status** of the power supply for the chosen device and the suggested action.

Step 7 Click **View Relevant Activities** for each stack identifier to view the **Activity Details** in the right pane.

Step 8 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The Machine Reasoning Engine (MRE) implements a system-end algorithm that detects and ends network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot a downed interface

Interface down troubleshooting workflow support is available only for these network devices with software version 16.9.3, and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the Cisco Catalyst Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see "Configure Role-Based Access Control" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **Interface Down** tab.

The **Interface Down** window displays the filtered list of devices with an interface that went down in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

Step 5 In the **Reasoner Input** window, enter the interface name that you suspect has issues.

Step 6 Click **Run Machine Reasoning**.

In the **Interface Down** window, you can see the **Root Cause Analysis** of the downed interface for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 7 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 8 Click the **Conclusion** tab to see the potential root causes for the interface down issue and the suggested action.

Step 9 Click **View Relevant Activities** for each root cause analysis to view the **Activity Details** in the right pane.

Step 10 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.



Note The Machine Reasoning Engine (MRE) implements a system-end algorithm that detects and ends network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot network connectivity

Only these network devices running Cisco IOS-XE software version 16.9.3 or later support the network connectivity troubleshooting:

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches

Use this procedure to check the reachability of an endpoint from a device using IP address:

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the Cisco Catalyst Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see "Configure Role-Based Access Control" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **Network Connectivity** tab.

Step 3 You can view the device table with details, such as **Device Name**, **IP Address**, **Device Type**, **Site**, **Reachability**, **Role**, and **Platform**.

Step 4 Select a device and click **Troubleshoot**.

Step 5 In the **Destination IP address** field of the **Reasoner Inputs** window, enter a valid IP address and click **Run Machine Reasoning**.

Note Provide the Virtual Routing and Forwarding (VRF) name, if applicable.

Step 6 In the **Root Cause Analysis** window, under **Reasoning Activity**, you can view various workflows that are validated as a part of the troubleshooting process.

Step 7 In the **Conclusions** tab, you can view the status of the validation check and the suggested action.

Troubleshoot IP connectivity of a device

As ping is a simple command, IP connectivity troubleshooting support is available for all the network devices.

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the Cisco Catalyst Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see "Configure Role-Based Access Control" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 In the **Network Reasoner** dashboard, click **Ping Device**.

Step 3 In the **Devices** window, choose a device and click **Troubleshoot**.

Step 4 In the **Reasoner Inputs** window, enter **Target IP Address** and click **Run Machine Reasoning**.

Step 5 Click **View Details** to view the ping status.

Troubleshoot wireless clients using the MRE workflow

Use this procedure to troubleshoot wireless client issues using the MRE workflow.

Note

- Wireless client troubleshooting workflow support is available only for network devices with Cisco IOS-XE software version 17.3.4 and later.
- The MRE workflow doesn't support HA, which means that if a switchover occurs during the workflow, you must repeat the workflow.

Before you begin

Make sure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **Wireless Client Data Collection** tile.
The **Devices** window shows the filtered wireless controller devices.

Step 3 Choose the wireless controller that you want to troubleshoot and click **Troubleshoot**.

Step 4 In the **Reasoner Inputs** window, complete these fields:

- **Troubleshoot Duration**
- **Client MAC Address**
- **PCAP Interface**: Click the drop-down arrow and choose an interface from the list. Use this option if packet capture is required.

Step 5 Click **Run Machine Reasoning**.
The **Wireless Client Data Collection** slide-in pane is displayed.

Step 6 In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process. Optionally, click **Stop** to stop the ongoing reasoning activity.

Step 7 Wait for the troubleshooting process to complete. After it completes, you can view the troubleshooting files under the **Conclusions** tab.

Step 8 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Step 9 (Optional) You can view the last troubleshooting files in the **Wireless Client Data Collection** slide-in pane when you start the wireless client troubleshooting workflow.

Troubleshoot wireless APs using the MRE workflow

Use this procedure to troubleshoot wireless AP issues using the MRE workflow.

Note

- Wireless AP troubleshooting workflow support is available only for network devices with Cisco IOS-XE software version 17.3.4 and later.
- The MRE workflow doesn't support HA, which means that if a switchover occurs during the workflow, you must repeat the workflow.

Before you begin

Make sure that the MRE knowledge base is updated with the latest knowledge packs. For more information, see "Update the Machine Reasoning Knowledge Base" in the Cisco Catalyst Center Administrator Guide.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **Wireless AP Data Collection** tile.

Step 3 The **Devices** window shows the filtered wireless controller devices. Choose the wireless controller device that you want to troubleshoot for the AP and click **Troubleshoot**.

Step 4 In the **Reasoner Inputs** window, complete these fields:

- **Troubleshoot Duration**
- **Two AP MAC Address**: Enter the AP MAC address for Ethernet and radio.
- If packet capture is required, use these options:
  - **PCAP Interface**: Click the drop-down list to choose the interface.
  - **AP IP Address**: Enter the AP IP address.
- **AP Name**

Step 5 Click **Run Machine Reasoning**.
The **Wireless AP Data Collection** slide-in pane appears.

Step 6 In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process. Optionally, click **Stop** to stop the ongoing reasoning activity.

Step 7 Wait for the troubleshooting process to complete. After it completes, you can view the troubleshooting files under the **Conclusions** tab.

Step 8 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Step 9 (Optional) You can view the last troubleshooting files in the **Wireless AP Data Collection** slide-in pane when you start the wireless AP troubleshooting workflow.

Troubleshoot unmonitored devices using the MRE workflow

Use this procedure to troubleshoot unmonitored devices or devices that are not showing Assurance data. The Troubleshooting Unmonitored Devices workflow supports only switches, Cisco AireOS Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controllers.

Before you begin

Make sure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Click the **Assurance Telemetry Analysis** tile.

Step 3 The **Devices** window shows the filtered unmonitored devices. Choose the device that you want to troubleshoot and click **Troubleshoot**.

The **Assurance Telemetry Analysis** slide-in pane is displayed. In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 4 Click **Stop** to stop the ongoing reasoning activity.

After the troubleshooting is complete, the **Machine Reasoning Completed** dialog box displays.

Step 5 Click **View Details**.

Step 6 You can view the troubleshooting files under the **Conclusions** tab. The issue is highlighted with an icon ( ), and the **Suggested Action** displays below the issue.

You can troubleshoot the unmonitored device with the suggestions provided.

Step 7 Click **Run Again** to rerun the troubleshooting process for the same device.

Step 8 You can also troubleshoot the devices from the **Inventory** tab. Scroll down to view the **Health Score** column. Click **No Health** under the **Health Score** column and click **View Assurance Telemetry Analysis** to run the troubleshooting process.

Troubleshoot HA on Cisco Wireless Controller using the MRE workflow

The MRE workflow analyzes the HA health on Cisco Wireless Controllers by processing the command outputs. This workflow is supported on the Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800-CL Wireless Controllers for Cloud running Cisco IOS XE Release 17.1 or later. Use this procedure to troubleshoot HA issues on wireless controllers using the MRE workflow.

Before you begin

Ensure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Alternatively, you can troubleshoot the HA issues on wireless controllers from the **Provision** > **Inventory** window. If there is an HA issue on a wireless controller, a red link icon ( ) is displayed next to the wireless controller. To troubleshoot the HA issues, click the red link icon, and then click **HA SSO Analysis**. Skip to Step 5, on page 1342.

Step 2 Click the **Catalyst 9800 Wireless Controller HA SSO Analysis** tile.
The **Devices** window displays the wireless controllers. If HA is configured on a wireless controller, Catalyst Center displays a link icon ( ) next to the device name. A red link icon ( ) indicates an HA issue on the wireless controller.

Step 3 From the left hierarchy tree, select the required site.

Step 4 Click the radio button next to the device name that you want to troubleshoot, and then click **Troubleshoot**.

Optionally, to stop the ongoing reasoning activity, click **Stop**.

Step 5 After the troubleshooting is complete, the **Machine Reasoning Completed** dialog box opens. Click **View Details**.

Step 6 In the **Root Cause Analysis** area, the **Reasoning Activity** tab displays the parameters that are checked as part of the troubleshooting process. To view the details of an activity, click the corresponding activity tile.

The analysis uses these parameters in the mentioned order:

Number	MRE analysis parameters	Description
1	**Check Controller Manageability**	• Checks if the wireless controller is running Cisco IOS XE Release 17.1 or later. • Checks if the wireless controller IP address is in reachable state. • Checks the SNMP, CLI credentials, and NETCONF. • Checks if the wireless controller is Cisco Catalyst 9800 Series Wireless Controllers or Cisco Catalyst 9800-CL Wireless Controllers for Cloud.
2	**Evaluate Catalyst Center platform**	Checks if all the services in the platform are a part of the Catalyst Center ISO.
3	**Check HA is configured in Controller**	Checks if the sensors on the active and standby wireless controller are operating in normal threshold range.
4	**Check Primary device and Secondary device status in HA Pair**	Checks if the HA configuration is completed on the wireless controllers.

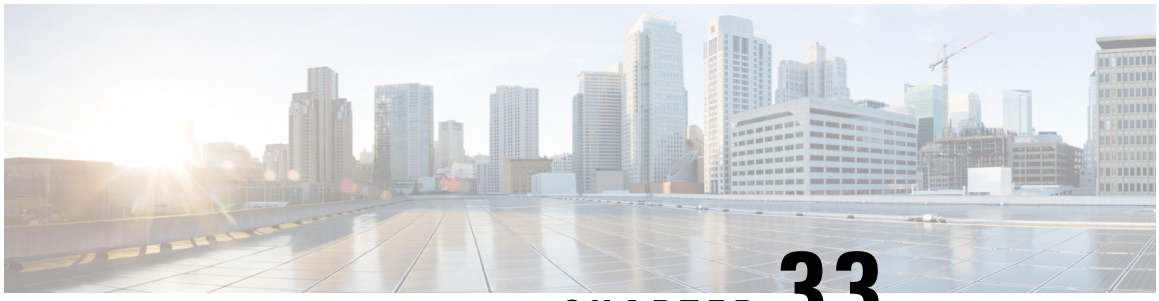
Number	MRE analysis parameters	Description
5	**Show RP and RMI status**	Checks the connectivity of the Redundancy Port (RP) link and Redundancy Management Interface (RMI) link between the active and standby wireless controllers running Cisco IOS XE Release 17.6 or later.
6	**Check the HA Status**	• Checks if the standby wireless controller is in HA removed state. • Checks if the standby wireless controller synchronization is in progress. • Checks if the power supply and RP network connectivity of the standby wireless controller are working as expected. • Checks if both active and standby wireless controllers are running the same image version.
7	**Secondary device deletion check**	• Checks if HA is configured successfully. • Checks if the standby wireless controller is in deleted state.

Step 7 The **Conclusions** tab displays the troubleshooting information. Catalyst Center highlights an issue with the ⚠ icon. It displays suggested action to resolve the issue in the **Suggested Action** area below the issue.

Step 8 (Optional) Click **Run Again** to rerun the troubleshooting process for the device.

What to do next

If your HA issue is not listed in the root cause or you need further assistance, contact Cisco Technical Assistance Center (TAC).



CHAPTER 33

Identify Network Bugs

- Network bug identifier tool overview, on page 1345
- Scan the network for bugs, on page 1346
- Scan Catalyst Center for bugs, on page 1347

Network bug identifier tool overview

The Catalyst Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.

The Catalyst Center network bug identifier helps in identifying specific patterns in the device configuration or in the operational data of the device and matches them with known defects based on those patterns. This tool provides both bug-focused and device-focused views.

Catalyst Center collects network device configuration and operational data by running CLI commands on network devices, and then sends the information to the CX Cloud to be processed for exposure to potential security advisories or bugs. Catalyst Center invokes these CLI commands for the network bug identifier tool:

- **show buffers summary**
- **show cef interfaces**
- **show clock**
- **show crypto eli all**
- **show crypto isakmp sa detail**
- **show eigrp service-family ipv4 neighbors**
- **show environment all**
- **show interfaces counters error**
- **show interfaces summary**
- **show inventory**
- **show ip interface brief**
- **show ip nat translations verbose**
- **show ip nbar protocol-discovery**

- **show ip nbar resources flow**
- **show ip nhrp**
- **show ip nhrp summary**
- **show ip route**
- **show ip ssh**
- **show ip vrf**
- **show logging**
- **show performance monitor cache detail**
- **show platform software route-map fp active map**
- **show pnp profile**
- **show redundancy**
- **show redundancy application group**
- **show running-config all**
- **show scp status**
- **show stackwise-virtual**
- **show startup-config**
- **show terminal**
- **show version**

Scan the network for bugs

Use this procedure to identify bugs using the network bug identifier tool.

Before you begin

- Install the Catalyst Center core package. For more information, see "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.
- Install the Machine Reasoning package. For more information, see "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Bug Identifier**.

Step 2 Click **Scan Network**.

Step 3 In the **Scan Network** window, select whether you want to scan your system for bugs **Now** or schedule it for **Later**.

The dashboard progress indicator shows the list of devices scanned in batches of 10. When the scan is done, the **Network Bug Identifier** window appears.

Step 4 Use the top pane to view information about the results of the scan, rescan the network, and change scan settings, as explained in this table:

Item	Description
Bug Summary	Number of **Catastrophic**, **Severe**, and **Moderate** bugs in your network.
Affected Devices	Number of device types that were scanned: • **Routers** • **Switches and Hubs**
Scan Mode	Method used to perform the scan: • **Essential**: Scan performed using the Cisco Network Reasoner Engine (NRE). • **CX Cloud**: Scan performed using the CX Cloud.
Re-scan Network	Click this button to scan your network again.
Settings	Click the **Settings** icon to do these tasks: • Enable or disable weekly scans. • Enable or disable the CX Cloud to scan your network.

Step 5 Click the **Bugs on Devices** tab to view information about the bug, such as **Bug ID**, **Name**, **Affected Devices**, **Severity**, **Affected Versions**, and **Workaround**.

Click any hyperlinked value to display more information about it.

Step 6 Click the **Devices** tab to view information about the devices, such as **Device Name**, **Image Version**, **IP Address**, **Device Type**, **Bugs**, **Scan Status**, **Scan Mode**, **Site**, and **Reachability**.

Click any hyperlinked value to display more information about it.

Step 7 From the **Devices** tab, click **Tag Device** to create, edit, or delete tags on the devices.

Scan Catalyst Center for bugs

The **System Bug Identifier** tool provides an option to identify bugs in the Catalyst Center. This procedure explains how to enable the **System Bug Identifier** tool:

Before you begin

- Install the Catalyst Center core package. For more information, see "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.

- Install the Machine Reasoning package. For more information, see "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Network Reasoner**.

Step 2 Select **System Bug Identifier**.

Step 3 Click **Scan System**.

Step 4 In the **Scan System** window, choose whether you want to scan your system for bugs **Now** or schedule it for **Later**.

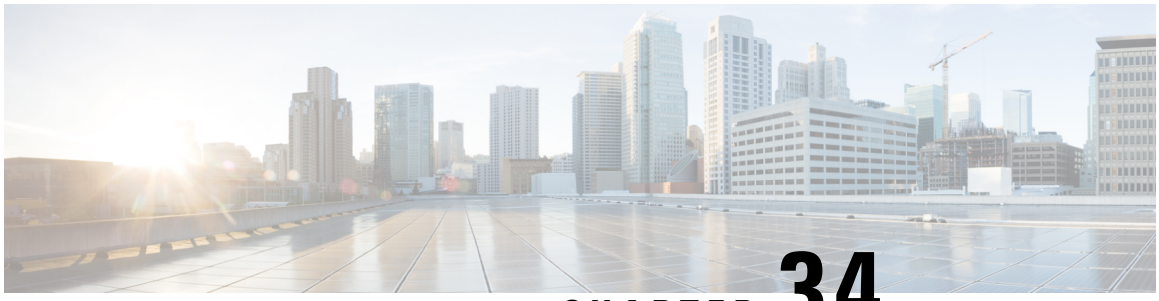
Note Click the **here** link in the banner that appears at the top of the window, to create new trial that provides access to customized bug information based on device configuration.

Step 5 The **System Bug Identifier** window shows the **BUG SUMMARY** and the **Bugs Identified on Your System** table.

In addition to basic bug information, this window shows information, such as when the bug was first and last identified, the frequency that it was identified and affected versions.

Step 6 Click the **Bug ID**.
The **Bug Details** dialog box displays the details of the bug.

Step 7 Click the arrow next to **Bug ID** to go to the **Bug Search Tools** window, which shows more details about the bugs.



CHAPTER 34

Identify Network Security Advisories

- Security advisories overview, on page 1349
- Prerequisites, on page 1350
- View security advisories, on page 1350
- Schedule a security advisories scan, on page 1352
- CLI commands invoked for security advisories, on page 1353
- Rescan the network to identify security advisories, on page 1353
- Hide and unhide devices from an advisory, on page 1354
- Hide and unhide advisories from a device, on page 1355
- Add notification for a security advisory knowledge bundle, on page 1355
- View security advisories in the inventory, on page 1356
- Live Protect Shields overview, on page 1357
- Complete the Live Protect Shields prerequisites, on page 1359
- Open the Live Protect Shields view, on page 1360
- Deploy a Live Protect Shield, on page 1360
- Switch between Monitoring and Enforcing modes, on page 1361
- Deploy a newer shield version, on page 1362
- Deactivate a Live Protect Shield, on page 1362
- View events and customize the table view, on page 1363
- Add a match pattern, on page 1363
- Define AND/OR for the match pattern, on page 1364
- Edit the match pattern, on page 1365
- Delete the match pattern, on page 1365

Security advisories overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends Cisco Security Advisories and Alerts.

The Security Advisories tool uses these recommended advisories, scans the inventory within Catalyst Center, and finds the devices with known vulnerabilities.

Prerequisites

To use the Security Advisories tool, you must install the Machine Reasoning package. See "Download and Install Packages and Updates" in the Cisco Catalyst Center Administrator Guide.

If you log in to Catalyst Center as an Observer, you cannot view the **Security Advisories** tool on the home page.

View security advisories

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Catalyst Center uses the knowledge base to identify security issues and improve automated analysis. We recommend that you update the knowledge base on a regular basis to view the latest security advisories.

a) From the main menu, choose **System** > **Settings** > **Machine Reasoning Engine**.
b) Either click **Import** or click **Download Latest** to download the latest available knowledge base. After the download, click **Import**.
c) Click the **AUTO UPDATE** toggle button to subscribe to automatic updates.

Note In the top banner, click the **here** link to create a new trial that provides access to customized field notices based on device configuration.

Step 3 The **ADVISORIES** area displays the distribution percentage of impact on the network, such as **Critical** or **High**.

Note The **Security Advisories** page no longer displays **Medium**, **Low**, or **Informational** advisories.

Step 4 Scans are done on the devices based on the licenses associated with each device. In the **SCAN CRITERIA** area, use this order to match advisories against your devices:

- **Software Version**: Scans are performed on devices based on the software version with an **Essentials** license.
- **Custom**: Scans are performed on devices based on the software version and the custom configuration entered for an advisory (if any) against the device running configuration with an **Advantage** license.
- **Advanced**: Scans are performed on devices based on the software version, configuration, and operations data on devices with **Cisco CX Cloud Success Track** entitlements.

  During the trial period, license entitlements are not enforced; all devices are scanned at the **Advanced** level.

Note

- The security advisories dashboard shows security advisories published by Cisco that may affect devices on your network based on the installed software image. A further analysis of the configuration, platform details, or other criteria is required to determine if a vulnerability is actually present.
- Security advisories scanning is only available for routers, switches, hubs, and wireless controllers that are running the minimum supported software version. For more information, see the Catalyst Center Compatibility Matrix.
- The security advisories displayed are subject to the Cisco Security Vulnerability Policy.

This table describes the information that is available.

Column	Description
Advisory ID	ID of the security advisory found in the network. Click the ID to go to the respective advisory web page.
Advisory title	Name of the security vulnerability advisory applicable to the network devices.
CVSS score	Score evaluated based on the Common Vulnerability Scoring System (CVSS) model.
Impact	Impact of the vulnerability on the network.
CVE	Common Vulnerabilities and Exposures (CVE) identifier for the vulnerability.
Devices	The number of devices impacted by the vulnerability. Click the number to view the devices that may be vulnerable based on this specific advisory, and upgrade the devices as needed.
Match Type	Indicates whether the vulnerability was detected based on the **Image Version** match or the **Configuration** match.
Known since (days)	The number of days since the vulnerability was discovered.
Last updated	The date when the advisory was last updated.

Step 5 The **FAILED DEVICES** area displays information about the device scan scheduled for a later date and time.

Note The **FAILED DEVICES** area appears only when there is a failed device in a scan and the system schedules a scan automatically.

Step 6 In the **Advisories** table, click the **All** tab to list all the advisories.

Step 7 In the **Advisories** table, click the **Affecting Devices** tab to view the advisories based on affecting devices.

Step 8 Click the **Devices** tab to view the number of advisories applicable to each device.

a) Click the number of advisories to view all that match the device.

b) Click the topology icon in the top-right corner to view the device topology. You can click a device in the topology to view all advisories that match the device.

A lock icon next to the device indicates that there are one or more advisories applicable to the device.

The **Fixed Version** column shows the version in which the advisories are fixed. You can remove the advisory on your device by upgrading to the version shown in this column.

Step 9 Click **Re-scan Network** to run the network scan again.

For information about the automated config scan, see Rescan the network to identify security advisories, on page 1353.

Schedule a security advisories scan

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 Click **Scan Network**.

The **Scan Network** window appears.

Step 3 To scan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 To schedule the scan for a later date and time, click the **Later** radio button and specify the date and time.

Step 5 Use the **Time Zone** drop-down list to schedule the scan according to a specific time zone.

Step 6 Choose the recurrence option: **None** (the default), **Daily**, or **Weekly**.

Step 7 In the **Run at Interval** field, enter the number of days or weeks for the recurrence of the scan.

Step 8 (Optional) Check the **Set Schedule End** check box to schedule an end date and number of occurrences.

a) To schedule a scan end date, click the **End Date** radio button and define the date and time.

b) To define the number of scan occurrences, click the **End After** radio button.

Step 9 Click **Schedule**.

Step 10 From the main menu, choose **Activities** > **Tasks** and confirm the schedule and recurrence of the scan.

Note In Catalyst Center releases earlier than 2.1.1.x, you have the ability to opt in or out of telemetry that Cisco collects. When you opt in, we collect your cisco.com ID, system telemetry, feature usage telemetry, network device inventory, and license entitlement. Telemetry is not application or feature specific; the disclosure of telemetry is for all of Catalyst Center. In Catalyst Center 2.1.1.x and later, telemetry collection is mandatory. The telemetry is designed to help the development of features that you use. See the *Cisco Catalyst Center Data Sheet* for a more expansive list of data that we collect.

When a security advisory scan runs, this telemetry data is collected:

- Whether automatic update of knowledge packages has been set up.
- Whether recurring scanning and recurring reports have been set up.
- The number of reports that have been run.
- The number of devices with a security advisory match based on software version and configuration.
- The number of thumbs up/thumbs down votes, per scan.
- The manual configurations entered as a search, and the associated advisory.
- The number of advisory matches by software version and configuration, including product family.
- The number of devices based on other categories (zero advisories, unknown, and unsupported).
- The number of successful, failed, and ended scans.
- The average scan time.

CLI commands invoked for security advisories

Catalyst Center collects network device configuration and operational data by running CLI commands on network devices, and then sends the information to the CX Cloud to be processed for exposure to potential security advisories or bugs. Catalyst Center invokes these CLI commands for security advisories:

- **show inventory**
- **show running-config**
- **show version**

Rescan the network to identify security advisories

Use this procedure to rescan the network to identify security advisories based on automated configuration scan.

Before you begin

You must enable the Cisco CX Cloud service. For more information, see **Update the Machine Reasoning Knowledge Base** in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories** > **Advisories**.

Step 2 Click **Re-Scan Network** to start the network scan again.

Step 3 To rescan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 To schedule the rescan for a later date and time, click the **Later** radio button and specify the details. For information, see Schedule a security advisories scan, on page 1352.

In the **Device** table, the **Advisories** column is updated with the number of advisories.

- The Catalyst Center network rescan sends the running config of devices along with other details, such as platform details and the CX Cloud software version. The information is processed and sent back to Catalyst Center. The Machine Reasoning Engine (MRE) running on Catalyst Center maps the advisories against the devices provided by the Cisco CX Cloud.
- If Catalyst Center cannot determine the correct license level for a given device, the security advisory scan falls back to scan by software version.

Hide and unhide devices from an advisory

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** window for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 To hide the devices from an advisory:

a) From the **Focus** drop-down list, choose **Advisories**.

b) In the **Devices** column, click the devices count that corresponds to the advisory for which you want to hide the devices.

The **Active** tab shows the number of devices for which these advisories are issued.

c) Choose the devices that you want to hide and click **Suppress Device**.

The hidden devices can be viewed in the **Suppressed** tab.

d) Close the advisory window and view the change in the device count for this advisory.

Step 5 To restore the devices to an advisory:

a) From the **Focus** drop-down list, choose **Advisories**.

b) In the **Devices** column, click the devices count that corresponds to the advisory for which you want to unhide the devices.

c) Click the **Suppressed** tab to view the hidden devices.

d) Choose the devices that you want to unhide and click **Mark as Active**.

The restored devices can be viewed in the **Active** tab.

e) Close the advisory window and view the change in the device count for this advisory.

Hide and unhide advisories from a device

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 To hide the advisories for a device:

a) From the **Focus** drop-down list, choose **Devices**.

b) In the **Advisories** column, click the advisories count that corresponds to device for which you want to hide the advisories.

The **Active** tab shows the number of advisories issued for this device.

c) Choose the advisories that you want to hide and click **Suppress Advisory**.

The hidden advisories can be viewed in the **Suppressed** tab.

d) Close the device window and view the change in the advisory count for this device.

Step 5 To restore the advisories for a device:

a) From the **Focus** drop-down list, choose **Devices**.

b) In the **Advisories** column, click the advisories count that corresponds to the device for which you want to unhide the advisories.

c) Click the **Suppressed** tab to view the hidden advisories.

d) Choose the advisories that you want to unhide and click **Mark as Active**.

The restored advisories can be viewed in the **Active** tab.

e) Close the device window and view the change in the advisories count for this device.

Add notification for a security advisory knowledge bundle

A security advisory knowledge bundle (KB) uses a Machine Reasoning Engine (MRE) to scan the network. You can configure Catalyst Center to notify you when a new security advisory KB is available. After you enable notifications, Catalyst Center displays a visual notification and actionable alert whenever a new security advisory KB is available.

Use this procedure to add notifications for new security advisory KBs:

Before you begin

- You must install the Catalyst Center core package. See "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.
- You must install the Machine Reasoning (MRE) package. See "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.
- These containers must be present in your system:
  - cnsr-reasoner
  - cloud connectivity/download

Procedure

Step 1 Click the notification icon in the top-right corner of the Catalyst Center GUI. From the drop-down menu, select the gear icon to view the notification preferences.

Step 2 In the **My Profile and Settings** window, enable the security advisory notification by choosing the **Security Advisories** option.

Step 3 Click **Save**.

Step 4 In the **Machine Reasoning Engine** window, click the **Download Latest** link to download the latest knowledge bundle.

Step 5 Review and update the Knowledge Base settings.

Step 6 In the **Security Advisory Settings** section, choose the recurrence option: **None** (default), **Daily**, or **Weekly**.

Step 7 Choose **Notification Center** > **Go to Security Advisories** to view the **Security Advisories** tool window directly.

Step 8 Rescan the network with the newly downloaded security advisories. For more information, see Schedule a security advisories scan, on page 1352.

View security advisories in the inventory

The Catalyst Center security focus view lists the security advisories for your devices, based on the data retrieved from the previous security scan. The device data that you retrieve from the **Security Advisories** tool is displayed in the **Inventory** window.

Use this procedure to view the security advisories:

Before you begin

- You must install the Catalyst Center core package. See "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.
- You must install the Machine Reasoning package. See "Download and Install Packages and Updates" in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 Click **Scan Network**.

Step 3 To scan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 From the main menu, choose **Provision** > **Network Devices** > **Inventory**.

Step 5 From the **FOCUS: Inventory** drop-down menu, select **Security**.
The **Advisories** column displays in the **Inventory** table.

Step 6 In the **Device Details** window, select a device and view the advisories data.

Step 7 Click **Manage All** to navigate to the **Security Advisories** tool.

Live Protect Shields overview

Live Protect Shields provide compensating controls that reduce your network's exposure to security vulnerabilities without device downtime.

When a Common Vulnerability and Exposure (CVE) is disclosed for Cisco IOS XE devices, a gap exists between disclosure and the availability or deployment of a full patch. Applying a full patch, such as a new IOS image or Software Maintenance Upgrade (SMU), typically requires a device reboot and downtime, which many organizations cannot accept. The Live Protect Shields feature maps to security advisories, while a security advisory maps to one or more CVEs.

Live Protect Shields close this gap by deploying lightweight shields (hot patches) that reduce exposure immediately, without service disruption, until permanent remediation through standard IOS XE patching can be completed. Each shield is associated with a specific security advisory and is deployed based on a combination of factors, including the impacted advisory and the target device family. The system may disrupt the service. Shields can cause side effects. The system logs and displays these side effects during shield deployment.

Supported device families

Live Protect Shields are supported on these Cisco Catalyst device families:

- Catalyst 9350
- Catalyst 9550
- Catalyst 9610
- Catalyst 9800

Shield states

State	Description
Available	The shield is ready to deploy but is not yet on the device. When you deploy and later deactivate a shield, the system displays it as available. The shield remains on the device, but the system does not activate it.
Monitoring	No protection. Monitoring logs vulnerability-related events without blocking them. The flagged operation is allowed to proceed and each occurrence is recorded as an event.
Enforcing	High protection. Enforcing blocks exploit attempts and logs them. The flagged operation is prevented from occurring and each occurrence is recorded as an event.
Failed	The shield deployment, mode switch, or deactivation did not complete successfully. Review the associated deployment task for details, and retry the operation.

Note

- Monitoring and Enforcing event totals are cumulative shield event totals. There is no separate deactivated state. When you deactivate a shield, the device returns to the Available state.
- Limitation: The "Not Applicable" status is not shown to users. The shield is on an advisory that does not impact your devices, or it targets a device family you do not have.
- Live Protect remains enabled at all times, except when in air-gap mode.

Shield deployment sidebar

The sidebar opens when you deploy, switch the mode of, or deactivate a shield, and provides detailed information about the shield, the associated advisory, and the current device status.

The sidebar includes an **About This Shield** area that summarizes what the selected shield does and the protection it provides. Use this information to understand the shield before you choose a deployment mode.

Table 74: Sidebar information

Field	Description
About This Shield	A summary of the shield and the protection it provides. It also details any potential side effects of the shield.
Advisory, Impact, and CVE	The associated security advisory, its impact level (for example, Critical or High), and the related CVE identifier.

Field	Description
Current Device Status	The current state of the shield on each device: Available, Monitoring, or Enforcing.
Current Events	The cumulative Monitoring and Enforcing event counts recorded for the shield on each device.
Current Shield Version	The version of the shield currently deployed on each device.
Deployed Time	The time at which the shield was deployed to the device.
Site and Device Details	The site and device information associated with each affected device.



Note The event totals in the **Current Events** area are cumulative shield event totals. An **Available** shield deploys no protection and therefore records no events, so event totals are only meaningful after a shield is deployed in Monitoring or Enforcing mode.

Live Protect Shields permissions

Live Protect Shields use the existing Security Advisories role and permission.

The default system roles **Super Admin** and **Network Admin** have write access to Security Advisories. Administrators can also create custom roles with read or write permissions to the Security Advisories function.

Permission	Capabilities
Write	Scan the network, deploy shields, switch modes, deactivate shields, and customize the table view.
Read	View shield states, events, and details only. The Scan Network button is grayed out, and action menus and the Settings icon are hidden.

Complete the Live Protect Shields prerequisites

How to complete the required setup steps before any Live Protect Shield information displays.

You must accept the license and run a security advisory scan before shields are populated for your devices.

Procedure

Run a security advisory scan before opening Live Protect Shields.

- Click **Scan Network** to run a scan manually.
- Rely on the automatic CX Cloud scan, which runs periodically.

For information about scan criteria and scan options, refer to View security advisories and Schedule a security advisories scan.

Open the Live Protect Shields view

Before you begin

Complete the prerequisites and run a security advisory scan.

You can access the Live Protect Shields view in three ways.

Procedure

Choose one of these navigation paths:

Path	Action
From the homepage	On the Catalyst Center homepage, click the **Live Protect Shields** tile.
From the menu	Go to **Tools** > **Security Advisories**, then click the **Live Protect Shields** tab.
From the summary totals or badge	Click a Live Protect summary event or the **New Versions Available** badge to open the **Live Protect Shields** tab with filters applied automatically.

The Live Protect Shields view displays only advisories that have a shield available or already deployed for your devices. If you accessed the view from a summary total or the **New Versions Available** badge, the table is filtered based on the selected value.

Deploy a Live Protect Shield

Install a shield on one or more devices that do not yet have it, and set the initial protection level.

Before you begin

- You must have write permission to Security Advisories.
- The shield must be in the Available state (not yet deployed) on the target devices.
- Maximum of 100 devices per deployment.

Procedure

Step 1 On the **Live Protect Shields** tab, locate the advisory row for the shield you want to install.

Step 2 Click the three-dot actions menu, then click **Deploy available**.

Step 3 In the sidebar, review the **About This Shield** summary, associated advisory, impact, and CVE.

Step 4 Select the **initial protection level**:

- **Monitoring** (default)— logs events without blocking.
- **Enforcing**— blocks exploit attempts and logs them.

Step 5 Select the target device or devices on which to deploy the shield.

Step 6 Click **Deploy Now**.

The shield is installed and begins recording events in the selected mode.

What to do next

To monitor progress, click the created task to open the **Activities** view, or click **Deployment Tasks** on the **Live Protect Shields** tab.

Switch between Monitoring and Enforcing modes

How to change the protection level of a deployed shield to balance event logging against the blocking of exploit attempts.

Before you begin

- You must have write permission to Security Advisories.
- The shield must already be in a **Monitoring**, or **Enforcing** state on at least one eligible device.

Procedure

Step 1 On the **Live Protect Shields** tab, locate the advisory row for the deployed shield.

Step 2 Click the three-dot actions menu, then click the transition that matches your goal:

Transition options	Result
Promote to Enforcing (from Monitoring)	Upgrades protection to block exploit attempts and log them.
Revert to Monitoring (from Enforcing)	Downgrades protection so events are logged without blocking.

Step 3 In the sidebar, review the current device status, current shield version, and cumulative events, then confirm the target mode.

Step 4 Select the target device or devices. You may select devices in mixed states in a single operation; only eligible devices are converted.

Step 5 Click **Deploy Now**.

Each selected device transitions to the target mode, and event totals continue to accumulate.

What to do next

Compare the cumulative events recorded across devices and modes to evaluate whether the current level of protection is sufficient. If Monitoring events continue to accumulate, consider switching the affected devices to Enforcing mode.

Deploy a newer shield version

How to deploy an improved version of a shield after it becomes available following a scan.

When the team improves a shield, a new version becomes available after the next scan. You cannot deploy an older version when a newer version exists; action menus are disabled for older versions.

Procedure

Step 1 On the **Live Protect Shields** tab, locate the newer version row.

Step 2 Click the three-dot actions menu on the newer version, then click **Deploy available**.

Step 3 Select the device or devices to receive the newer version.

Step 4 Click **Deploy Now**.

The newest version appears as the parent row, older versions appear as expandable child rows, and deploy actions are available only on the newest version. Deploying the newer version replaces the current shield on selected devices.

Deactivate a Live Protect Shield

How to remove protection from a device and return the shield to the Available state.

Before you begin

You must have write permission to Security Advisories.

Deactivating a shield returns the device to the same condition it was in before the shield was deployed. You can redeploy the shield later if needed.

Procedure

Step 1 Click the three-dot actions menu for the deployed shield.

Step 2 Select the **Deactivate** option.

Step 3 Select the device or devices that currently have the shield deployed.



Note Only devices that currently have the shield deployed appear in the deactivation list.

Step 4 Confirm the deactivation.

The shield is deactivated on the device, and the device returns to the **Available** state.

View events and customize the table view

How to review the events recorded by deployed shields and save a personalized table layout.

Events represent the number of times a flagged operation occurred on a device. Events are only recorded after a shield is deployed; an Available shield records no events.

Procedure

Step 1 To view events, locate the device on the **Advisory ID** row and review the **Events** column. For device-level event details, open the deployment sidebar to view the **Device details**.

The Events column displays Monitoring events (operations allowed and recorded) and Enforcing events (operations blocked and recorded).

Step 2 (Optional) To customize the table view, click the **Settings** icon in the last column.

Note The Settings icon is only available to users with write permission.

Step 3 (Optional) Adjust your preferences, such as row density and displayed columns. A live preview shows your changes.

Step 4 (Optional) Click **Apply** to save.

Saved table preferences are stored per user and persist across sessions, even after you log out.

Add a match pattern

To see which devices are and aren't impacted by advisories under specific device conditions, add a match pattern to an advisory before running a network scan.

When running a new network scan, Catalyst Center first checks if the device software version matches the software version described in the advisory. If the versions don't match, the match pattern for the advisory is ignored. If the versions match, Catalyst Center checks for a match between the device configuration and match pattern. If there is a match, the impacted advisory is attached to the impacted devices. If there is not a match, the impacted advisory is detached from the impacted devices.

Note This feature applies to a network scan using only basic scan criteria.

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** window for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory and in the **Match Type** column, click **Add match pattern**.

Step 5 In the **Add Configuration Match Pattern** window, enter the condition to match with devices in the **CONDITIONS** text box.

Step 6 Click **Save**.

The match pattern is added to the advisory.

Step 7 Click **Scan Network**.

The **Devices** table displays the scanned device results when the **Scanned** filter is chosen.

Define AND/OR for the match pattern

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory and in the **Match Type** column, click **Add match pattern**.

Step 5 In the **Add Configuration Match Pattern** window, do these steps:

a) In the **CONDITIONS** text box, enter a condition and then click the **Add** icon.

b) From the drop-down list, select **AND** or **OR** and then enter the next condition.

c) If you want to delete a condition, click the **Remove** icon.

d) Click **Save**.
The match pattern is added to the advisory.

Step 6 Click **Scan Network** to check the number of devices that match the match pattern.

Edit the match pattern

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory that already has a match pattern and in the **Match Type** column, click **Edit match pattern**.

Step 5 In the **Edit Configuration Match Pattern** window, enter the condition to match with devices in the **CONDITIONS** text box.

Step 6 Click **Save**.

The match pattern is changed.

Step 7 Click **Scan Network** to check the number of devices that match the match pattern.

Delete the match pattern

Procedure

Step 1 From the main menu, choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

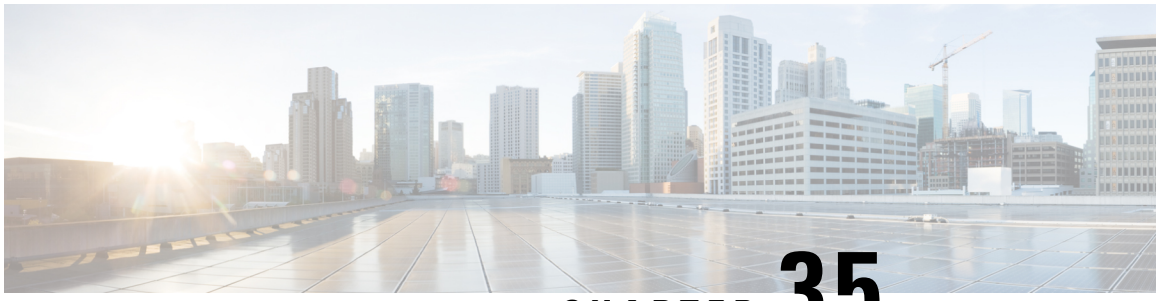
Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory that already has a match pattern and in the **Match Type** column, click **Edit match pattern**.

Step 5 In the **Edit Configuration Match Pattern** window, click **Delete**.

The match pattern is deleted.

Delete the match pattern



CHAPTER 35

Identify Network Field Notices

- Field Notices identifier tool overview, on page 1367
- View Field Notices, on page 1367

Field Notices identifier tool overview

Field Notices are notifications that are published for significant issues, other than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

The Field Notices tool uses these notifications, scans the inventory within Catalyst Center, and finds the devices with these known issues.

View Field Notices

Procedure

Step 1 From the main menu, choose **Tools** > **Field Notices**.

Step 2 If you are launching the **Field Notices** window for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, do these steps:

a) If required, edit the default **Task Name**.

b) Click **Now** to scan the network immediately, or click **Later** to scan the network at a later time.

Note In the top banner, click the **here** link to create a new trial that provides access to customized field notices based on device configuration.

Step 4 On completion of the scan, the **FIELD NOTICES** area displays the field notices for hardware and software issues. To view the list of devices and the issues identified for the devices, click the **Devices** tab and do these steps:

a) In the **SUMMARY** area, expand **Devices Family** and filter the device family (**Routers**, **Switches and Hubs**, **Unified AP**, or **Wireless Controller**).

b) Expand **Scan Status** and filter the devices based on **Success**, **Failed**, or **Not Scanned**.

The **Devices** table displays the list of devices based on **Device Name**, **IP Address**, **Device Family**, **Site**, **Field Notices**, **Potential Field Notices**, **Scan Status**, **Last Scanned**, **Site**, and **Reachability**.

The **Field Notices** and **Potential Field Notices** columns display the number of field notices and potential field notices for the device.

c) Click a number from the respective column to open a slide-in pane with additional details.

d) In the slide-in pane, click the **Field Notices** or **Potential Field Notices** tab to view a table with additional information.

Note The **Reason** column is shown only for potential field notices.

e) (Optional) Click the **Details** tab to view hardware, software details, and operational summary.

Step 5 Click the **Field Notices** tab and do these steps:

a) In the **SUMMARY** area, expand **Field Notice Type**.

b) Choose the type **Hardware** or **Software**.

The **Field Notices** table displays with additional information.

c) The **Affected Devices** column displays the number of affected devices. Click a number to open a slide-in pane with additional details.

Affected devices meet all the criteria that can be checked automatically for a field notice. No additional manual verification is required to confirm that the device is affected.

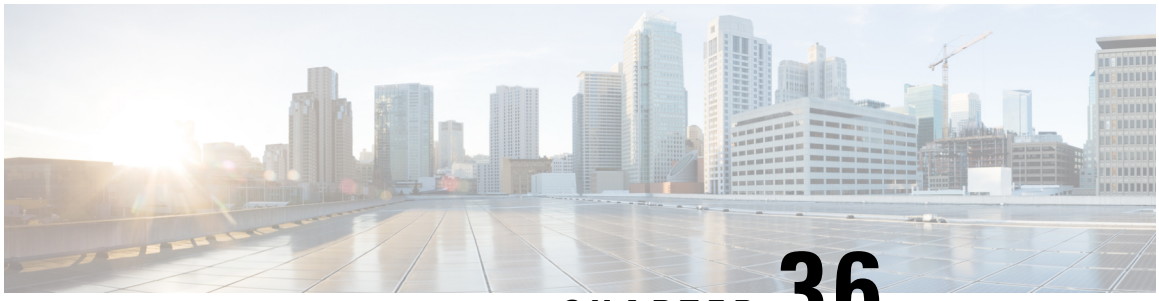
d) The **Potentially Affected Devices** column displays the number of potentially affected devices. Click a number to open a slide-in pane with additional details.

Potentially affected devices meet all the criteria that can be checked automatically for a field notice; however, additional manual verification is required to confirm that the device is affected.

Step 6 (Optional) Click **Re-scan Network** to run the network scan again.

a) In the **Scan Network** slide-in pane, choose whether you want to scan your system for field notices **Now** or **Later**, and click **Submit**.

b) To view the progress, click the menu icon and choose **Activities** > **Tasks** and confirm the schedule and recurrence of the scan.



CHAPTER 36

Generate the Root Cause Analysis File from Catalyst Center

- Support Bundle overview, on page 1369
- Collect and upload provisioning failure root cause analysis data, on page 1369

Support Bundle overview

The Support Bundle enables the collection of more modular and granular root cause analysis (RCA) data for different services. The RCA data includes relevant information specific to the selected service in addition to the cluster's metadata, such as node information, Catalyst Center version, packages, disaster recovery status, package release version, and so on.

Collect and upload provisioning failure root cause analysis data

This procedure shows how to collect root cause analysis (RCA) data from a provisioning failure and upload the RCA data to a Cisco TAC service request (SR).

Procedure

Step 1 From the top-right corner, click the help icon and choose **Support Bundle**.

Step 2 Click **Create Support Bundle**.

Step 3 In the **Create Support Bundle** slide-in pane, enter a name and description for the support bundle.

Step 4 Select the time period for which you're requesting support, and select the system category.

Step 5 From the **Application** drop-down list, select the applicable support bundle.

Step 6 Expand **Have Cisco Personnel Requested Any Additional Parameters?** and enter any additional parameters to optimize the RCA collection.

Step 7 Click **Submit**.

Step 8 Under the **Actions** column, click the download icon to download the newly created support bundle.

The support bundle RCA file downloads in .tar.gz file format.

Step 9 To upload the RCA file to a Cisco TAC service request, under the **Actions** column, click the upload icon.

Step 10 In the **RCA Upload - Generate CLI** window, do these tasks:

- Enter the **SR Number**.
- Enter the **File Upload Token**.
- Click **Generate CLI Commands**.
- Click **Copy** to copy the CLI commands.

Step 11 Log in to the Catalyst Center CLI and paste the CLI commands at the CLI shell prompt.



PART VIII

Manage Catalyst Center

- Build and Deploy Workflows, on page 1373
- Wireless Network Configuration Use Cases, on page 1427
- Manage Energy on Your Network, on page 1455
- Troubleshoot Catalyst Center Using Data Platform, on page 1467
- Proactive Remediation for Discovered Issues, on page 1471



CHAPTER 37

Build and Deploy Workflows

- Catalyst Center workflow navigation, on page 1373
- Discover devices, on page 1374
- AP Refresh workflow, on page 1375
- Enable application hosting on switches, on page 1378
- Enable IoT services, on page 1380
- AP configurations in Catalyst Center, on page 1382
- Replace a device, on page 1407
- Switch refresh, on page 1413
- Create a remote support authorization, on page 1415
- Create an event notification, on page 1416
- Configure Remote LAN, on page 1420
- Configure Parallel Redundancy Protocol in a fabric site, on page 1423

Catalyst Center workflow navigation

Catalyst Center workflows are similar to wizards. The workflows are embedded in the GUI to guide you through multistep tasks that would otherwise be too complex or advanced to complete. You can access many of them from various menu options or directly from the **Workflows** menu option.

Use these guidelines to help you navigate through the workflows:

- Follow the steps in the workflow and click **Next** to go to the next page.
- When you hover your cursor near the top of each page in the workflow, a **Progress bar** displays, showing you the steps to complete the process and which step you are currently on.
- Some workflows open a dialog box that you can click through to see a visual overview of the task. At any point in the task overview, you can click **Let's Do it** to jump directly to the beginning of the workflow.

  To skip the task overview in the future, check the **Don't show this to me again** check box.
- In the bottom-left corner, click **Exit** to leave a workflow. Then in the confirmation dialog box, click **Exit**. Your progress is saved automatically, and the **Workflows** window displays the workflow in-progress card for the task.
- On the **Workflows** window, hover your cursor over the bottom-right corner ellipsis in a workflow in-progress card and click **Resume** to resume that workflow.

Discover devices

This workflow guides you from device discovery to network health.

Before you begin

- Your devices must have the required device configurations, as described in Discovery prerequisites, on page 56.
- Enable CDP on your network devices, if you want to use CDP discovery protocol.
- Enable LLDP on your network devices, if you want to use LLDP discovery protocol.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Procedure

Step 1 From the main menu, choose **Workflows** > **Discover Devices**.

Step 2 If a task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 3 In the **Discover Devices** window, complete these fields:

a) Enter a name for the discovery job.

b) Under **Discovery Type**, choose the protocol used to discover devices and complete the corresponding fields:

- **CDP**: Enter the **IP Address**, **CDP Level**, and **Subnet Filter**.
- **IP Address Range**: Enter the **Starting IP Address** and **Ending IP Address**.
- **LLDP**: Enter the **IP Address**, **LLDP Level**, and **Subnet Filter**.

c) Choose the **Preferred Management IP Address**.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential for Catalyst Center to configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see Discovery credentials, on page 57.

a) In the left pane, click **CLI** to add CLI credentials.

b) Expand **SNMP** to add SNMP credentials.

c) Expand **Advanced Settings** and configure these settings:

Setting	Task
Protocol Order	Select **SSH** or **Telnet**. If you select both, you can specify the order in which they are used by dragging the protocols up or down.
SNMP Polling Properties	Use the global SNMP polling properties defined in the **Network Settings** > **Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF, HTTP, and HTTPS, if required.

Step 5 In the **Schedule Job** window, do these steps:

a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you select the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

b) Click the toggle button to enable or disable the **Discover new devices only** option.

c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box appears with information about the settings that enable on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview is not generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, select any one of these options:

Option	Task
Assign to site without Configuration Preview	Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see Search the network hierarchy, on page 240.
Skip site assignment for now	Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities** > **Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

AP Refresh workflow

The AP Refresh feature allows you to replace both provisioned and unprovisioned older AP models with newer AP models, using the Access Point Refresh workflow. You can use this procedure to replace old APs with new ones in Catalyst Center for these use cases:

- Automation use case: Deployments where wireless controller and APs are provisioned through Catalyst Center network intent configurations. After AP refresh, the new AP is provisioned with the network intent configuration.

- Assurance or Campus Automation use case: Deployments where Catalyst Center is used primarily for Assurance purposes and the wireless controller and APs are not provisioned through Catalyst Center network intent configurations. The new AP isn't provisioned after AP refresh and only the old configuration is copied to the new AP.

For device compatibility information, see the *Catalyst Center Compatibility Matrix*.

Before you begin

- Ensure that the old AP is assigned to a site.
- The new AP must not be assigned to any site.
- For the automation use case, the old AP site must be provisioned as a managed AP location for the wireless controller to which the new AP is associated.
- For the Assurance or Campus Automation use case, the new AP must join the same wireless controller where the old AP was previously associated.
- For the automation use case, you must connect the new AP to a wireless controller. The new AP must either be available in the Catalyst Center inventory or be able to contact Catalyst Center through Plug and Play (PnP). It must be in the Reachable state.
- For the Assurance or Campus Automation use case, you must connect the new AP to a wireless controller. The new AP must be available in the Catalyst Center inventory or be able to contact Catalyst Center through Plug and Play (PnP). It must be in the Reachable state.

Procedure

Step 1 From the main menu, choose **Workflows** > **Access Point Refresh**.

Note If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 2 In the **Before you begin** window, view the prerequisites for the AP refresh workflow.

Step 3 In the **Get started** window, enter a unique name for the task.

Step 4 In the **Select your scenario** window, click the radio button next to the required use case: **Automation Use Case** or **Assurance/Campus Automation Usecase**

Step 5 In the **Select Access Points** window, do these steps:

a. In the left pane, check the check box next to the floor where you want to refresh the AP.

b. In the right pane, check the check box next to the device name that you want to replace.

Step 6 In the **Assign New APs to Old APs** window, do these steps:

a) (Optional) By default, automatic detection of new APs through the switch port is enabled. If necessary, you can disable automatic detection of new APs using the toggle button.

Ensure that the Cisco Discovery Protocol (CDP) is enabled on the wireless controller or AP for automatic detection of new APs.

Note Automatic detection of new APs through the switch port isn't supported when it’s onboarded through PnP.

When you enable the automatic detection of new APs, this workflow does these tasks:

- If the new AP is connected to the same switch port where the old AP is connected, the serial number of the new AP is automatically populated.
- If the new AP isn’t onboarded yet, the serial number of the new AP is detected after it’s discovered. Alternatively, you can enter the serial number of the new AP.

b) Select a method through which you want to provide new AP details:

- To add the new AP details using the GUI, click the edit icon ( ) for the AP, and in the **Edit details** window, do these steps:

  1. (Optional) Update the new AP name.
  2. (Optional) From the **Choose Platform ID** drop-down list, choose the platform of the new AP.
  3. From the **Choose Serial Number** drop-down list, choose the serial number of the new AP.

     If the new AP is already associated with a wireless controller and is available in the inventory, Catalyst Center displays the serial number of that AP as **Managed** in the **Choose Serial Number** drop-down list.

     If the new AP has contacted Catalyst Center through PnP, Catalyst Center displays the serial number of that AP as **Unclaimed** in the **Choose Serial Number** drop-down list.

     If the serial number of the new AP isn’t available in the Inventory, the **Serial Number** drop-down list doesn’t contain the serial number. To add a new serial number that isn’t present in the inventory, from the **Choose Serial Number** drop-down list, enter the serial number and click **+**.

     Note If you enable the automatic detection of new APs using SwitchPort, choosing the serial number is optional.

  4. Click **Save**.

- To add the new AP details using a comma-separated value (CSV) file, do these steps:

  1. Click **Download CSV**. The downloaded CSV template file contains the old AP details. Update the device name and add the serial number of the new AP.
  2. To import the CSV file, click **Upload CSV**.
  3. In the **Upload CSV** window, you can either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.

     Catalyst Center performs a validation check. If the uploaded CSV file doesn’t meet the requirement, an error message is displayed. Click **View Details** to get more details about the error message.
  4. Click **Upload**.

Step 7 In the **Configuration to be copied from Old APs to New** window, view the configuration that will be copied from the old AP to the new AP.

Step 8 In the **Schedule Access Point Refresh Task** window, click **Now** or **Run Later** to schedule the AP refresh task for a later date and time.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 In the **Track Replacement Status** window, monitor the AP replacement status:

- If the AP replacement succeeds, the **Replacement Status** shows **REPLACED**.
- If the AP replacement fails, the **Replacement Status** shows **Error**.



Note If the new AP isn't yet discovered in the inventory and the corresponding AP refresh entry is waiting for the new device to be connected, or if the PnP claim process is in progress, resynchronize the Cisco Wireless Controller.

Step 11 (Optional) In the **Track Replacement Status** window, do any of these tasks:

- To view the latest AP replacement status, click **Refresh Data**.
- To delete a replacement entry, click **Delete**. In the **Warning** dialog box, click **Yes**.
- If there is any error during replacement, click **Retry** to retrigger replacement.
- To download the provisioning status report, click **Download Report**.

Step 12 Click **Next** to view the refresh summary.

You can view the status of the task in the **Activities** > **Tasks** window.

After a successful replacement, an AP refresh event is generated in Cisco Catalyst Assurance for the old and new APs.

Step 13 (Optional) View the AP refresh event under **Event Viewer** in the **AP View 360** window.

Catalyst Center automatically updates the new APs on the respective floor maps in the **Network Hierarchy** window.

Enable application hosting on switches

Use this procedure to enable docker applications such as ThousandEyes Enterprise Agent and iPerf in selected switches at a specific site.

Before you begin

- Complete the prerequisites. For more information, see Prerequisites for application hosting, on page 1135.
- Add the application to Catalyst Center. For more information, see Add an application, on page 1139.
- Check the readiness of the switch to host the application. For more information, see View device readiness to host an application, on page 1136.

Procedure

Step 1 From the main menu, choose **Provision** > **Services** > **Application Hosting**.

Step 2 Choose the application and click **Install** at the bottom of the window.

Alternatively, you can also launch the workflow by choosing **Workflows** > **Enable Apps on Switches** > **Let's Do it**.

Note At the top of the workflow window, place your cursor on the blue progress bar and switch back to the previous step listed.

Step 3 In the **Select Site** window, navigate to the building where you want to enable the application.

Step 4 In the **Select App** window, click on the application you want to select.

Note You can access the **+ New App** link to add an application that is not present in Catalyst Center.

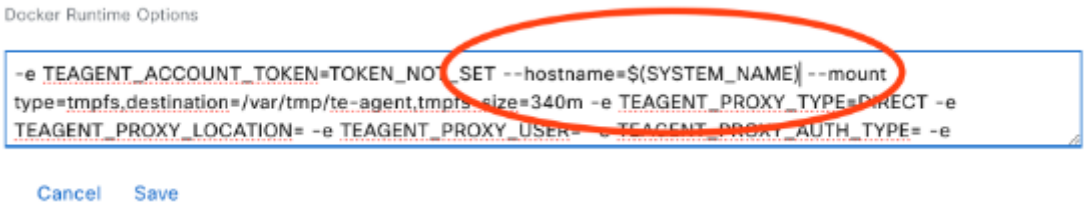
Step 5 In the **Select Switches** window, check the check box next to the device name for which you want to enable the application.

Note You can import or export devices in bulk by providing the details in the specified template in the **Select Switches** dialog box.

Step 6 Complete these settings in the **Configuration App** window:

- **App Networking**
  - **Device Network**: From the **Select Network** drop-down list, choose a VLAN to configure the application.
  - **App IP address**: From the **Address Type** drop-down list, choose **Static** or **Dynamic**. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.
- **Resource Allocation**: Check the **Allocate resources as asked by the app** or the **Allocate all resources available on the device** check box.
- **Custom Settings**: (Applicable only for Cisco package applications) Enter the configuration details for the attributes that are specified by the application.
- **App Data**: Browse and upload the application-specific files. To identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options**: Enter the docker runtime options required by the application.

Important For ThousandEyes application, by default the docker runtime option mentions the hostname as a variable $(SYSTEM_NAME).



The variable $(SYSTEM_NAME) must be added with a domain name, as a Fully Qualified Domain Name (FQDN) is required. The FQDN consists of two parts, a hostname and the domain name.

You must manually add the domain name to the variable $(SYSTEM_NAME) in the format $(SYSTEM_NAME).domain.name. The variable $(SYSTEM_NAME) will be automatically replaced by the device hostname after deployment.

For example, if the FQDN of the device is *ise.cisco.com*, here the hostname is "ise" and the domain name is "cisco.com". In the docker runtime option you must manually add "cisco.com" to the variable; $(SYSTEM_NAME).cisco.com. The variable will be automatically replaced with "ise" after deployment.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

The **Provisioning Task** window displays the task name that tracks the deployment of the application on the switches.

Step 8 Review the automatically generated task name and click **Provision**.

Step 9 In the **Track Provisioning Status** window, you can track the progress of the deployment.

Step 10 Click **View Details** to view the provisioning status of the individual devices and failures, if any and click **Next**.

The application is enabled successfully.

The summary of the task result and the success/failure counts display.

Step 11 Click **Manage App**, where you can manage the lifecycle operations of the application to perform day-*n* tasks.

Enable IoT services

These sections provide information about enabling IoT technologies such as Bluetooth, Zigbee, and ESL on Cisco Catalyst 9100 Series Access Points using **Workflows** in Catalyst Center.

Enable IoT services on Cisco Catalyst 9100 Series Access Points

This procedure shows how to enable IoT technologies such as Bluetooth, Zigbee, and ESL on selected Catalyst 9100 Series Access Points.

Procedure

Step 1 From the main menu, choose **Workflows** > **Enable IOT Services**.

Step 2 If a task overview window opens, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Select Site** window, navigate to the floor where you want to enable the IoT service, and click **Next**.

Step 4 In the **Select the Application** window, select the SES-imagotag ESL Connector application to enable IoT in your network, and click **Next**.

Note To add an application that is not present in the Catalyst Center, see Add an Application.

The **Select Access Points** window shows all the APs available on the particular floor.

Step 5 In the **Select Access Points** window, check the check box adjacent to the **Device Name** where you want to install the IoT connector application, and click **Next**.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 The **Provisioning Task** window, which displays the task name created to track deployment of any application on APs, displays. Review the auto-generated task name and click **Provision**.

Step 8 In the **Track Provisioning Status** window, you can track the progress of the deployment. Click **View Details** to view the provisioning status and click **Next**.

Step 9 The **Done! Task Completed** window displays. Click **Manage IoT Application** to do day-*n* tasks.

Manage IoT applications

Use this procedure to manage IoT applications.

Before you begin

You must have enabled IoT services on Cisco Catalyst 9000 Series Access Points.

Procedure

Step 1 After enabling IoT services, click **Manage IoT Application** in the **Done! Task Completed** window.

Step 2 Check the check box next to the **Hostname** and do these tasks:

- To start the application, from the **Actions** drop-down list, choose **Start App**.
- To stop the application, from the **Actions** drop-down list, choose **Stop App**.
- To edit the application configuration, from the **Actions** drop-down list, choose **Edit App Config**.
- To upgrade the application, from the **Actions** drop-down list, choose **Upgrade App**.
- To uninstall the application from the selected AP, from the **Actions** drop-down list, choose **Uninstall App**.

Step 3 Click the AP name to view details, such as the AP name, status, IP address, and health.

Step 4 Click **Tech Support logs** to collect Application Hosting logs.

AP configurations in Catalyst Center

Use the **Configure Access Points** workflow for these tasks:

- Configure and deploy AP-level and radio-level parameters on APs. See Configure APs, on page 1382.
- Schedule recurring events for APs. See Schedule recurring events for APs, on page 1400.
- Configure APs using existing templates. See Configure APs using existing templates, on page 1403.

Configure APs

Use this procedure to configure AP and radio parameters in Catalyst Center.

These settings configured using the **Configure Access Points** workflow aren't overwritten when the wireless controller or APs are reprovisioned:

- Admin status for radios (only applicable for Cisco AireOS Wireless Controllers)
- AP primary controller
- AP secondary controller

Note The AP configuration is generated from the information available in the Catalyst Center inventory. To ensure that the latest configuration is generated, complete an inventory sync on the controller.

For parameters that include the **Enable**, **Disable**, and **No-Change** options, use each option as described:

- **Enable**: Enable the parameter.
- **Disable**: Disable the parameter.
- **No-Change**: Keep the AP state unchanged for the parameter.

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure Access Points**.

If the **Configure Your Access Points** dialog box displays, click **Let's Do It** to go directly to the workflow.

Step 2 In the **Get Started** window, enter a unique name for the workflow in the **Task Name** field and click **Next**.

Step 3 In the **Select configuration method** window, configure the AP and radio parameters.

a) Click the **Configure AP and Radio Parameters** radio button.

b) From the **Apply template** drop-down list, choose **No-Change**.

Note To configure APs and radio parameters using an existing template, refer to Configure APs using existing templates, on page 1403.

c) Check the check box next to the tasks that you want to do:

- **Modify AP Name**
- **Configure AP Geolocation Parameters**
- **Configure AP Parameters**
- **Configure AP LAN port parameters**
- **Configure 5 GHz Radio Parameters**
- **Configure 2.4 GHz Radio Parameters**
- **Configure 6 GHz Radio Parameters**
- **Configure Dual-Band (XOR) Radio Parameters**
- **Configure Tri-Radio Parameters**
- **Create and Save a Reusable Template for Selected Configurations(s)**

Note Based on the check boxes that you check, Catalyst Center displays the corresponding subsequent configuration steps.

d) Click **Next**.

Step 4 In the **Select Access Points** window, choose the APs that you want to configure.

a) Choose the assigned APs or unassigned APs that you want to configure.

If you chose the...	Then...
Assigned APs tab	Navigate to the site where you want to apply AP-related configurations. The right pane lists all APs available in the selected site. **Note** You can choose up to 2,000 sites in this window.
Unassigned APs tab	Check the **Unassigned Devices** check box. The right pane lists all APs that aren't assigned to any site.

b) Select APs that you want to configure.

Note You can select up to 4,000 APs in this window, including both APs that are assigned to a site and unassigned APs.

To select the APs, use one of these methods:

- To select individual APs, check the check boxes next to the AP names.
- To select all APs displayed on the page, check the check box at the top of the table.

  By default, 100 rows are displayed per page.
- To select all APs across multiple pages, check the check box at the top of the table and click **Select All** that appears.

  Note This option is available only if the total number of APs does not exceed 4,000.
- Use the filter fields available on top of each column to filter the APs based on the required criteria. After filtering, check the check box at the top of the table to select all APs on the page that match the search criteria, or check the check boxes next to the required AP names.

c) (Optional) To customize the **Access Points** table, click the gear icon in the top-right corner of the table and use these options:

- Under **Table density**, choose the preferred table density.
- Under **Table columns**, check the check boxes next to the column names that you want to display in the table.

d) Click **Next**.

Step 5 If you chose APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, click the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue With The Workflow	Continue with the workflow. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box and choose different APs in the **Select Access Points** window.

Step 6 (Optional) In the **Modify AP Name** window, modify one or more AP names using one of these options.

If you want to...	Then...
update AP name individually	in the corresponding **New AP Name** field, update the AP name.
apply a naming pattern (for example, *AP-###*) and generate sequential names for all listed APs	enter a name based on your naming convention, and click **Apply Pattern**.
update AP names using a CSV template	complete these steps: **a.** Click **Export CSV** to download the CSV file with the current AP names. **b.** Update the AP names in the CSV file. **c.** Click **Import CSV**. **d.** Browse to choose the updated CSV file. **e.** Click **Open**.

Step 7 (Optional) In the **Configure AP Geolocation Parameters** window, configure the geolocation parameters for eligible APs.

Geolocation parameters are used for features like Automated Frequency Coordination (AFC). These parameters are available for only the APs that are running Cisco IOS XE Release 17.12 or later.

Note To use the 6-GHz band at standard power, you must configure geolocation parameters and enable the **Standard Power Service** toggle button in the RF profile. For more information, see Create a wireless radio frequency profile, on page 383.

This window lists the reachable APs that support geolocation parameters.

If you want to...	Then...
filter the APs	you can either: • click **Search**, enter a value, and then press the **Enter** key, or • enter any combination of values in the available **Filter** fields for the table columns. For example, you can enter values in the AP Name, Ethernet MAC Address, and Site fields.
filter the APs based on standard power configuration status	click the **All**, **Enabled**, or **Disabled** toggle button.

If you want to...	Then...
configure height	complete these steps: **a.** Check the check box next to the required APs. **b.** Click **Configure Height from Ground**. **c.** In the **Height (m)** field, enter the height from the ground in meters (rounded to the nearest whole number). The valid range is from -100 to 1000. **d.** In the **Height Uncertainty (m)** field, enter the height uncertainty in meters. The valid range is from 1 to 100. **Note** Higher height uncertainty can lead to lower accuracy of power limits reported by AFC. **e.** (Optional) If APs are connected through an antenna cable, in the **Cable Length (m)** field, enter the cable length in meters. The valid range is from 1 to 100. **Note** If the AP doesn't support this data, this field is dimmed. **f.** (Optional) Check the **Apply these settings to selected Access Points on Unassigned** to apply these settings to other unassigned APs selected in the **Select Access Points** window. **Note** Cable length is not applied to APs that do not have 6-GHz radio.
download the data in CSV format	complete these steps: **a.** Check the check box next to the required APs. **b.** Click **Download CSV**.

If you want to...	Then...
upload the data for multiple APs in CSV format	complete these steps: **a.** Check the check box next to the required APs. **b.** Click **Upload CSV**. **c.** In the Warning dialog box, click **Yes**. **d.** In the **Upload CSV** dialog box, you can either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file. **Note** This CSV file must have the same format as the downloaded CSV file. **e.** Click **Upload**.

Step 8 (Optional) In the **Configure AP Parameters** window, configure these AP parameters:

a) Under **General**, complete these configurations:

- Choose the required option for **Admin Status**: **Enable**, **Disable**, or **No-Change**.
- From the **AP Mode** drop-down list, select the required option.

  Valid modes are **Local/Flexconnect**, **Monitor**, **Sniffer**, and **Bridge/Flex+Bridge**. To keep the AP mode unchanged, select **No-Change**.

  When AP mode is enabled, the VLAN tag, bridge role, and RAP downlink backhaul options are dimmed. This option is dimmed when the VLAN tag option is enabled.

Note When you change the AP mode from **Monitor** or **Sniffer** to **Local/Flexconnect**, Catalyst Center uses these settings:

- If **FlexConnect Local Switching** is enabled on any associated SSID, Catalyst Center sets **FlexConnect** mode on the AP. Otherwise, it sets the **Local** mode on the AP.
- For unassigned APs or the assigned APs aren't provisioned, Catalyst Center sets **FlexConnect** mode on the AP based on the device:
  - For Cisco AireOS Wireless Controller: If **FlexConnect Local Switching** is enabled on any associated SSID in the AP group where the AP is present.
  - For Cisco Catalyst 9800 Series Wireless Controller: If **Local site** is disabled on the current associated site tag of the AP.
- Configure the AP mode, VLAN tag, and bridge role in separate workflows as these parameters cause the AP to reboot.

For information about mesh networks, see About wireless mesh networks, on page 449.

- From the **Bridge Role** drop-down list, choose the required option to configure mesh role (Mesh Access Point or Root Access Point) for the AP.

  The **Applicable APs** field shows how many APs support mesh role configuration, which is only available for APs with per-device configuration (not intent-based APs).

  Configure the bridge role, VLAN tag, and AP mode in separate workflows as these parameters cause the AP to reboot.

  Note When this option is enabled, the VLAN tag and RAP downlink backhaul options are dimmed. This option is dimmed when the VLAN tag or RAP downlink backhaul option is enabled.

- From the **RAP Downlink Backhaul** drop-down list, choose the downlink backhaul radio band for Root Access Point (RAP) in bridge role.

  Catalyst Center displays the number of applicable APs. If applicable APs are available, click the number to view AP details.

  Note When this option is enabled, the bridge role and VLAN tag options are dimmed. This option is dimmed when the bridge role or VLAN tag option is enabled.

- From the **AP Location** drop-down list, select the required option.
  - To use the currently assigned site as the AP location, select **Use currently assigned site location**.

  Note If you check the **Use currently assigned site location check box**, for APs that aren’t assigned to any site, Catalyst Center doesn't configure the AP location.

  - To enter a custom location, select **Custom Location**. In the **Enter Location** field, enter the AP location details.

  Note If you do not enter the AP location in the **Enter Location** field, the default value *default-location* is used.

  - To keep the AP location unchanged, select **No-Change**.

  You can view the AP location that is being configured for each AP by clicking **View location details** before pushing this change to the device.

b) Under **CleanAir Pro / CleanAir / Spectrum Intelligence**, choose an option to configure the CleanAir spectrum intelligence for the 2.4-GHz, 5-GHz, or 6-GHz radio bands: **Enable**, **Disable**, or **No-Change**.

Note You can configure CleanAir spectrum intelligence only on CleanAir spectrum intelligence-capable APs that are in the **Local/FlexConnect** or **Monitor** modes. If CleanAir spectrum intelligence is disabled on the 802.11a network, the operational status is down for the AP.

c) Under **LED & Hardware**, complete these configurations:

- Select the required option for **AP LED Status**: **Enable**, **Disable**, or **No-Change**.
- From the **LED Brightness Level** drop-down list, choose the brightness level.

  To keep the LED brightness level unchanged, select **No-Change**.
- Choose the required option for **Accelerometer**: **Enable**, **Disable**, or **No-Change**.

  The accelerometer provides tilt data to monitor AP orientation.

  When the accelerometer is enabled, Catalyst Center displays the AP tilt information in the inventory.

  Catalyst Center displays the number of applicable APs. If applicable APs are available, click the number to view AP details.

  The accelerometer feature is available only on Cisco Catalyst 9166D1 Series APs, Cisco Catalyst 9176I Series Access APs, Cisco Catalyst 9176D1 Series APs, and Cisco Catalyst 9178I Series APs.

Note Resynchronize the wireless controller to display the sensor tilt details in the inventory. For more information, see Resynchronize device information, on page 182.

d) Under **High Availability**, complete these configurations.

- Configure the primary, secondary, and tertiary controller name and the IP address for the AP.

  From the controller name drop-down list, choose the required option. To keep this AP configuration unchanged, choose **No-Change**. If you choose **Inherit from site / Clear** for the primary and secondary controllers:

  - For the APs that are in Provisioned state, the controllers that are configured as primary and secondary for the floor where the AP is assigned are configured as the primary and secondary controllers on the AP.
  - For the APs that aren’t in Provisioned state, the current primary and secondary controller configuration is cleared from the AP.

  For the tertiary controller, the **Clear** option is available.

Note

- If AP fallback is disabled on the controller, the AP doesn't join the newly configured primary, secondary, and tertiary controller.
- If the AP is a ROW AP, ensure that you have added support for the country of operation to the country list on the controller. You must configure at least one site from the country of operation as the managed AP location for the controller.

- From the **AP Failover Priority** drop-down list, choose a failover priority.
  - **Low**: Level 1 priority, which is the lowest priority level.
  - **Medium**: Level 2 priority.
  - **High**: Level 3 priority.
  - **Critical**: Level 4 priority, which is the highest priority level.
  - **No-Change**: Keep the AP failover priority unchanged.

e) Under **VLAN**, complete these configurations.

- Choose the required option for **VLAN Tag** to allow multiple VLANs to be managed on a single port: **Enable**, **Disable**, or **No-Change**.



Note
- VLAN tag configuration is not applicable for APs in Bridge mode.
- Configure the VLAN tag, AP mode, and bridge role in separate workflows as these parameters cause the AP to reboot.
- When this option is enabled, the bridge role and RAP downlink backhaul options are dimmed. This option is dimmed when the AP mode, bridge role, or RAP downlink backhaul options is enabled.

- In the **VLAN Tag ID** field, enter the tag. The valid range is from 1 to 4094.



Note This field is available only when the VLAN tag configuration is enabled.

f) Under **Domain Name System Configuration**, configure Domain Name System (DNS) for APs with static IP addresses:

- In the **DNS Server** field, enter the IP address of the server.

  You can enter an IPv4 or IPv6 address, but ensure that the IP address is reachable from the static IP address configured on the AP.

- In the **Domain Name** field, enter the domain name.

Step 9 (Optional) In the **Configure AP LAN port parameters** window, configure the AP LAN port parameters for applicable APs.

- For LAN1, LAN2, and LAN3, choose the required option: **Enable**, **Disable**, or **No-Change**.
- If you enabled the LAN1 port, under **PoE Status**, choose the required option for Power over Ethernet (PoE) for the port.

  When you enable PoE, the USB module is automatically disabled on the device.



Note If you chose APs that are associated with a wireless controller that is managed using site-based network profiles, you can't configure the AP LAN port parameters.

Step 10 (Optional) In the **Configure 5 GHz Radio Parameters** window, configure the 802.11 a/n/ac/ax parameters.

a) Under **General**, complete these configurations:

- Choose the required option for **Admin Status**.
- Choose the required option for **Radio Role Assignment**.

  Valid roles are **Auto**, **Client-Serving**, or **Monitor**. To keep the radio role unchanged, select **No-Change**.

  To view the list of applicable APs for the 5-GHz radio parameter configuration, click **View Devices**. Catalyst Center displays the **View Devices** option only when APs that support the 5-GHz radio parameters are available.

b) Under **Antenna Parameters**, complete these configurations:

- From the **Antenna Gain** drop-down list, choose an antenna.

  If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 to 40.



Note The selected antenna name isn't reflected in wireless maps.

- From the **Antenna Cable** drop-down list, choose an antenna cable to compute the effective gain.

  If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 to 40.



Note This option is unavailable if the radio role assignment is **Monitor**.

c) Under **RF Parameters**, complete these configurations:



Note **RF Parameters** configurations are available only when the radio role is **Client-Serving**.

- Choose the required option for **Power Assignment**.

  To choose a custom power value, select **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

  To keep the power assignment unchanged, select **No-Change**.

- Choose the required option for **Channel Assignment**.

To choose custom channel numbers, select **Custom**. If you choose **Custom**, complete these configurations:

- From the **Select Custom Channel** drop-down list, choose a custom channel number.
- (Optional) From the **Channel Width** drop-down list, choose a channel width.

To keep the channel assignment unchanged, select **No-Change**.

d) Under **BSS Color**, Choose the required option for **BSS Color Configuration** to configure BSS color for applicable APs:

- To configure BSS color at the global level, select **Global**.
- To configure custom BSS color, select **Custom**.

  Under **BSS Color Radio Admin Status**, choose the required option.

  If you enable the BSS color radio admin status, in the **BSS Color Code** field, enter the BSS color code. The valid range is from 1 to 63.
- To keep the BSS color configuration unchanged, select **No-Change**.

Note For APs associated with Cisco AireOS Wireless Controller, enabling BSS color on this band enables the BSS color at the global level, which may cause network disruptions.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design** > **Network Hierarchy** window. For more information, see Edit an AP, on page 269.

Step 11 (Optional) In the **Configure 2.4 GHz Radio Parameters** window, configure the 2.4-GHz radio parameters.

a) To view the list of applicable APs for the 2.4-GHz radio parameter configuration, click **View Devices**.

Catalyst Center displays the **View Devices** option only when APs that support the 2.4-GHz radio parameters are available.

b) Under **General**, complete these configurations:

- Choose the required option for **Admin Status**: **Enable**, **Disable**, or **No-Change**.
- Choose the required option for **Radio Role Assignment**.

  Valid roles are **Auto**, **Client-Serving**, or **Monitor**. To keep the radio role unchanged, select **No-Change**.

Note This option is dimmed if an unsupported AP is selected in the **Select Access Points** window.

c) Under **Antenna Parameters**, complete these configurations:

- From the **Antenna Gain** drop-down list, choose an antenna.

  If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 to 40.

  Note The selected antenna name isn't reflected in wireless maps.

- From the **Antenna Cable** drop-down list, choose an antenna cable.

  If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 to 40.

  Note This option is unavailable if the radio role assignment is **Monitor**.

d) Under **RF Parameters**, complete these configurations:

Note **RF Parameters** configurations are available only when the radio role is **Client-Serving**.

- Choose the required option for **Power Assignment**.

  To choose a custom power value, select **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

  To keep the power assignment unchanged, select **No-Change**.

- Choose the required option for **Channel Assignment**.

  To choose custom channel numbers, select **Custom**. Choose a custom channel number from the **Select Custom Channel** drop-down list.

  To keep the channel assignment unchanged, select **No-Change**.

e) Under **BSS Color**, choose the required option for **BSS Color Configuration** to configure BSS color for applicable APs:

- To configure BSS color at the global level, select **Global**.
- To configure custom BSS color, select **Custom**.

  Under **BSS Color Radio Admin Status**, choose the required option.

  If you enable the BSS color radio admin status, in the **BSS Color Code** field, enter the BSS color code. The valid range is from 1 to 63.

- To keep the BSS color configuration unchanged, select **No-Change**.

Note For APs associated with Cisco AireOS Wireless Controller, enabling BSS color on this band enables the BSS color at the global level, which may cause network disruptions.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design** > **Network Hierarchy** window. For more information, see Edit an AP, on page 269.

Step 12 (Optional) In the **Configure 6 GHz Radio Parameters** window, configure the 6-GHz radio parameters.

a) To view the list of applicable APs for the 6-GHz radio parameter configuration, click **View Devices**.

Catalyst Center displays the **View Devices** option only when APs that support the 6-GHz radio parameters are available.

b) Under **General**, complete these configurations:

- Choose the required option for **Admin Status**: **Enable**, **Disable**, or **No-Change**.
- Choose the required option for **Radio Role Assignment**.

  Valid roles are **Auto**, **Client-Serving**, or **Monitor**. To keep the radio role unchanged, select **No-Change**.

c) Under **BSS Color**, choose the required option for **BSS Color Configuration** to configure BSS color for applicable APs:

- To configure BSS color at the global level, select **Global**.
- To configure custom BSS color, select **Custom**.

  Under **BSS Color Radio Admin Status**, choose the required option.

  If you enable the BSS color radio admin status, in the **BSS Color Code** field, enter the BSS color code. The valid range is from 1 to 63.
- To keep the BSS color configuration unchanged, select **No-Change**.

Note For APs associated with Cisco AireOS Wireless Controller, enabling BSS color on this band enables the BSS color at the global level, which may cause network disruptions.

d) Under **RF Parameters**, complete these configurations:

Note **RF Parameters** configurations are available only when the radio role is **Client-Serving**.

- Choose the required option for **Power Assignment**.

To choose a custom power value, select **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

To keep the power assignment unchanged, select **No-Change**.

- Choose the required option for **Channel Assignment**.

  To choose custom channel numbers, select **Custom**. To keep the channel assignment unchanged, select **No-Change**.

  If you choose **Custom**, complete these configurations:

  - From the **Select Custom Channel** drop-down list, choose a custom channel number.
  - (Optional) From the **Channel Width** drop-down list, choose a channel width.

Note The 320-MHz channel width is available only for the Wi-Fi 7 APs: Cisco Catalyst 9172H Series Access Points, Cisco Catalyst 9172I Series Access Points, Cisco Catalyst 9176D1 Series Access Points, Cisco Catalyst 9176I Series Access Points, and Cisco Catalyst 9178I Series Access Points.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design** > **Network Hierarchy** window. For more information, see Edit an AP, on page 269.

Step 13 (Optional) In the **Configure Dual-Band (XOR) Radio Parameters** window, configure the dual-band (XOR) radio parameters.

a) To view the list of applicable APs for the XOR radio parameter configuration, click **View Devices**.

Catalyst Center displays the **View Devices** option only when APs that support XOR parameters are available.

You can configure XOR radio parameters on these APs:

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9166 Series Access Points
- Cisco Wireless 9171I Series Access Points running Cisco IOS XE Release 17.18 or later
- Cisco Wireless 9174I Series Access Points running Cisco IOS XE Release 17.18 or later
- Cisco Wireless 9174E Series Access Points running Cisco IOS XE Release 17.18 or later
- Cisco Catalyst 9176D1 Series Access Points running Cisco IOS XE Release 17.15 or later
- Cisco Catalyst 9176I Series Access Points running Cisco IOS XE Release 17.15 or later

- Cisco Wireless 9177D Series Access Points
- Cisco Wireless 9177E Series Access Points
- Cisco Wireless 9177I Series Access Points
- Cisco Catalyst IW9165E Access Points
- Cisco Catalyst IW9165D Heavy Duty Access Points
- Cisco Catalyst IW9167E Heavy Duty Access Points

Note Cisco Catalyst 9166 Series Access Points and Cisco Wireless 9171I Series Access Points support XOR between 5-GHz and 6-GHz radio modes. The other APs support XOR between 2.4-GHz and 5-GHz radio modes.

b) Under **General**, complete these configurations:

- Choose the required option for **Admin Status**: **Enable**, **Disable**, or **No-Change**.
- Choose the required option for **Radio Role Assignment**.

  Valid roles are **Auto**, **Client-Serving**, or **Monitor**. To keep the radio role unchanged, select **No-Change**.

  (Optional) For the **Client-Serving** role, choose the 2.4-GHz, 5-GHz, or 6-GHz radio band from the available options.

Note For AP models with external antenna, you can choose the 5-GHz radio band only when the Directional Antenna Radio Terminal (DART) connector is connected.

c) Under **Antenna Parameters**, complete these configurations for the 2.4-GHz radio band:

- From the **Antenna Gain** drop-down list, choose an antenna.

  If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 to 40.

Note The selected antenna name isn't reflected in wireless maps.

- From the **Antenna Cable** drop-down list, choose an antenna cable.

  If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 to 40.

Note This option is unavailable if the radio role assignment is **Monitor**.

d) Under **RF Parameters**, complete these configurations:

Note **RF Parameters** configurations are available only when the radio role is **Client-Serving**.

- Choose the required option for **Power Assignment**.

  To choose a custom power value, select **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

  To keep the power assignment unchanged, select **No-Change**.

- Choose the required option for **Channel Assignment**.

  To choose custom channel numbers, select **Custom**. To keep the channel assignment unchanged, select **No-Change**.

  If you choose **Custom**, complete these configurations:

  - From the **Select Custom Channel** drop-down list, choose a custom channel number.
  - (Optional) From the **Channel Width** drop-down list, choose a channel width.

Note Channel width is not applicable for the 2.4 GHz radio band. If the dual radio mode is enabled on an XOR-capable AP, its slot 2 can't be in the **Client-Serving** radio role with the 160-MHz channel width.

e) Under **BSS Color**, Choose the required option for **BSS Color Configuration** to configure BSS color for applicable APs:

- To configure BSS color at the global level, select **Global**.
- To configure custom BSS color, select **Custom**.

  Under **BSS Color Radio Admin Status**, choose the required option.

  If you enable the BSS color radio admin status, in the **BSS Color Code** field, enter the BSS color code. The valid range is from 1 to 63.

- To keep the BSS color configuration unchanged, select **No-Change**.

Note For APs associated with Cisco AireOS Wireless Controller, enabling BSS color on this band enables the BSS color at the global level, which may cause network disruptions.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design** > **Network Hierarchy** window. For more information, see Edit an AP, on page 269.

Step 14 (Optional) In the **Configure Tri-Radio Parameters** window, configure the tri-radio parameters.

a) To view the list of applicable APs for the tri-radio parameter configuration, click **View Devices**.

Note
- Catalyst Center displays the **View Devices** option only when APs that support tri-radio parameters are available.
- Catalyst Center doesn't support tri-radio parameter configuration for APs that are in **Monitor** or **Sniffer** modes.

You can configure tri-radio parameters on these APs:

- Cisco Catalyst 9124AXE Series Access Points
- Cisco Catalyst 9130AXI Series Access Points
- Cisco Catalyst 9130AXE Series Access Points
- Cisco Catalyst 9178I Series Access Points
- Cisco Catalyst 9179F Series Access Points

b) Under **General**, complete these configurations:

- Choose the required option for **Dual Radio Mode**.

  Valid modes are **Auto**, **Enable**, or **Disable**. To keep the dual radio mode unchanged, select **No-Change**.

  Note When you enable dual radio mode, global tri-radio mode is enabled on the corresponding wireless controllers.

- Choose the required option for **Radio Role Assignment**.

  Valid roles are **Auto**, **Client-Serving**, or **Monitor**. To keep the radio role unchanged, select **No-Change**.

  Note This option is available only if the dual radio mode is enabled.

- Choose the required option for **Admin Status**: **Enable**, **Disable**, or **No-Change**.

  Note This option is available only if the dual radio mode is enabled.

c) Under **Antenna Parameters**, complete these configurations:

- From the **Antenna Gain** drop-down list, choose an antenna.

  If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio

energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 to 40.

Note The selected antenna name isn't reflected in wireless maps.

- From the **Antenna Cable** drop-down list, choose an antenna cable.

  If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 to 40.

Note This option is unavailable if the radio role assignment is **Monitor**.

d) Under **RF Parameters**, complete these configurations:

Note **RF Parameters** configurations are available only when the radio role is **Client-Serving**.

- Choose the required option for **Power Assignment**.

  To choose a custom power value, select **Custom**. Choose the power level from the **Select Custom Power** drop-down list.

  To keep the power assignment unchanged, select **No-Change**.

- Choose the required option for **Channel Assignment**.

  To choose custom channel numbers, select **Custom**. To keep the channel assignment unchanged, select **No-Change**.

  If you choose **Custom**, complete these configurations:

  - From the **Select Custom Channel** drop-down list, choose a custom channel number.
  - From the **Channel Width** drop-down list, choose a channel width.

e) Under **BSS Color**, Choose the required option for **BSS Color Configuration** to configure BSS color for applicable APs:

- To configure BSS color at the global level, select **Global**.
- To configure custom BSS color, select **Custom**.

  Under **BSS Color Radio Admin Status**, choose the required option.

  If you enable the BSS color radio admin status, in the **BSS Color Code** field, enter the BSS color code. The valid range is from 1 to 63.

- To keep the BSS color configuration unchanged, select **No-Change**.

Note For APs associated with Cisco AireOS Wireless Controller, enabling BSS color on this band enables the BSS color at the global level, which may cause network disruptions.

Note The **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure these parameters in the **Design** > **Network Hierarchy** window. For more information, see Edit an AP, on page 269.

Step 15 (Optional) In the **Save As Reusable Template** window, choose an option.

- To save as a new template, click **Create** and enter a name for the template in the **Template Name** field. By default, the **Template Name** field is autofilled with the workflow name. You can use the same name or change as required.

  (Optional) In the **Description** field, enter a description.

  Note The maximum number of templates supported is 500.

- To skip the template creation, click **Do Not Save**.

Step 16 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 17 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Note If you chose to save this configured workflow as a new template, it's created when you click **Configure**.

Step 18 On the **Tasks** window, monitor the task deployment.

Schedule recurring events for APs

Use this procedure to schedule recurring events for AP and radio parameters in Catalyst Center.

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure Access Points**.

If the **Configure Your Access Points** dialog box displays, click **Let's Do It** to go directly to the workflow.

Step 2 In the **Get Started** window, enter a unique name for the task in the **Task Name** field.

Step 3 In the **Select configuration method** window, click the **Schedule Recurring Events For AP and Radio Parameters** radio button.

Step 4 In the **Select Access Points** window, choose the APs that you want to configure.

a) Choose the assigned APs or unassigned APs that you want to configure.

If you chose the...	Then...
Assigned APs tab	Navigate to the site where you want to apply AP-related configurations. The right pane lists all APs available in the selected site. **Note** You can choose up to 2,000 sites in this window.
Unassigned APs tab	Check the **Unassigned Devices** check box. The right pane lists all APs that aren't assigned to any site.

b) Select APs that you want to configure.

Note You can select up to 4,000 APs in this window, including both APs that are assigned to a site and unassigned APs.

To select the APs, use one of these methods:

- To select individual APs, check the check boxes next to the AP names.
- To select all APs displayed on the page, check the check box at the top of the table.

  By default, 100 rows are displayed per page.
- To select all APs across multiple pages, check the check box at the top of the table and click **Select All** that appears.

  Note This option is available only if the total number of APs does not exceed 4,000.
- Use the filter fields available on top of each column to filter the APs based on the required criteria. After filtering, check the check box at the top of the table to select all APs on the page that match the search criteria, or check the check boxes next to the required AP names.

c) (Optional) To customize the **Access Points** table, click the gear icon in the top-right corner of the table and use these options:

- Under **Table density**, choose the preferred table density.
- Under **Table columns**, check the check boxes next to the column names that you want to display in the table.

d) Click **Next**.

Step 5 If you chose APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, click the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, refer to "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.
Continue With The Workflow	Continue with the workflow. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box and choose different APs in the **Select Access Points** window.

Step 6 In the **Select AP and Radio Parameters** window, select the required option for each AP and radio parameter.

- **Enable**: Enable the parameter.
- **Disable**: Disable the parameter.
- **No-Change**: Keep the AP state unchanged for the parameter.

Catalyst Center applies certain settings to only one of the AP slots, including:

- **5 GHz Admin Status**: Applied to slot 1 of the applicable APs.
- **2.4 GHz Admin Status**: Applied to slot 0 of the applicable APs.
- **6 GHz Admin Status**: Applied to these slots:
  - Slot 3 of the 6-GHz-capable Cisco Catalyst 9136 Series APs, Cisco Catalyst 9178I Series APs, and Cisco Catalyst 9179F Series APs.
  - Slot 2 of the 6-GHz-capable Cisco Catalyst 9162 Series APs, Cisco Catalyst 9162 Series APs, Cisco Catalyst 9164 Series APs, Cisco Catalyst 9172H Series Access Points, Cisco Catalyst 9172I Series Access Points, Cisco Catalyst 9176D1 Series Access Points, Cisco Catalyst 9176I Series Access Points, and Cisco Catalyst IW9167I Heavy Duty APs.
- **Dual-Band (XOR) Admin Status**: Applied to slot 0 of these dual-band (XOR)-capable APs:
  - Cisco Aironet 2800 Series Access Points
  - Cisco Aironet 3800 Series Access Points

- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9176D1 Series Access Points
- Cisco Catalyst 9176I Series Access Points

Applied to slot 1 of the dual-band (XOR)-capable Cisco Wireless 9171I Series APs.

Applied to slot 2 of these dual-band (XOR)-capable APs:

- Cisco Catalyst 9166 Series APs
- Cisco Catalyst IW9165E APs,
- Cisco Catalyst IW9165D Heavy Duty APs
- Cisco Catalyst IW9167E Heavy Duty APs
- Cisco Wireless 9174I Series Access Points
- Cisco Wireless 9174E Series Access Points.
- Cisco Wireless 9177D Series Access Points
- Cisco Wireless 9177E Series Access Points
- Cisco Wireless 9177I Series Access Points

- **Tri-Radio Admin Status**: Applied to slot 2 of the tri-radio-capable APs with dual radio mode enabled.

To disable the configuration of a parameter, check the corresponding check box and click **Disable**.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 9 On the **Tasks** window, monitor the task deployment.

Configure APs using existing templates

Use this procedure to configure AP and radio parameters in Catalyst Center using an existing template.

Before you begin

Ensure that AP configuration templates are available. To create a new template, choose the **Create Template** option in the **Configure AP And Radio Parameters** workflow. For more information, see Configure APs, on page 1382.

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure Access Points**.

If the **Configure Your Access Points** dialog box displays, click **Let's Do It** to go directly to the workflow.

Step 2 In the **Get Started** window, enter a unique name for the workflow in the **Task Name** field.

Step 3 In the **Select configuration method** window, complete these configurations:

a) Click the **Configure AP and Radio Parameters** radio button.

b) From the **Apply template** drop-down list, select the template.

c) (Optional) To manage templates, click **Manage templates**.

In the **Manage templates** slide-in pane, complete these configurations:

If you want to...	Then...
View the configurations in a template	**1.** Click the template name. You can filter the data based on the template name and description using the corresponding field. **2.** View the configurations. **3.** Click **Back** to return to the **Manage templates** slide-in pane.
Delete templates	**1.** Check the check box next to the required templates. To select all templates, click **Select All**. **Note** You cannot delete a template that is already applied. **2.** Click **Delete**. **3.** In the **Warning** dialog box, click **Delete**.

Step 4 In the **Select Access Points** window, choose the APs that you want to configure.

a) Choose the assigned APs or unassigned APs that you want to configure.

If you chose the...	Then...
Assigned APs tab	Navigate to the site where you want to apply AP-related configurations. The right pane lists all APs available in the selected site. **Note** You can choose up to 2,000 sites in this window.

If you chose the...	Then...
Unassigned APs tab	Check the **Unassigned Devices** check box. The right pane lists all APs that aren't assigned to any site.

b) Select APs that you want to configure.

Note You can select up to 4,000 APs in this window, including both APs that are assigned to a site and unassigned APs.

To select the APs, use one of these methods:

- To select individual APs, check the check boxes next to the AP names.
- To select all APs displayed on the page, check the check box at the top of the table.

  By default, 100 rows are displayed per page.
- To select all APs across multiple pages, check the check box at the top of the table and click **Select All** that appears.

  Note This option is available only if the total number of APs does not exceed 4,000.
- Use the filter fields available on top of each column to filter the APs based on the required criteria. After filtering, check the check box at the top of the table to select all APs on the page that match the search criteria, or check the check boxes next to the required AP names.

c) (Optional) To customize the **Access Points** table, click the gear icon in the top-right corner of the table and use these options:

- Under **Table density**, choose the preferred table density.
- Under **Table columns**, check the check boxes next to the column names that you want to display in the table.

d) Click **Next**.

Step 5 If you chose APs that don't meet the license requirements, Catalyst Center displays a dialog box with the details. In the dialog box, click the required option.

Option	Description
License Manager	Open the **License Manager** window and enable the corresponding licenses. To enable the licenses, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Option	Description
Continue With The Workflow	Continue with the workflow. **Note** APs that don't meet the license requirements are in worldwide safe mode (WWSM).
Cancel	Close the dialog box and choose different APs in the **Select Access Points** window.

Step 6 Based on the configuration settings in the selected template, Catalyst Center displays the corresponding subsequent configuration windows. Each of these configuration windows displays the preconfigured settings according to the template. You can choose to continue with existing configurations or reconfigure as required. For more information on configuring the AP and radio parameters, see Configure APs, on page 1382.

Note In the **Modify AP Name** window, the list of APs displayed is based on the APs that you selected previously on the **Select Access Points** window and not according to the template settings.

- **Modify AP Name**
- **Configure AP Geolocation Parameters**
- **Configure AP Parameters**
- **Configure AP LAN port parameters**
- **Configure 5 GHz Radio Parameters**
- **Configure 2.4 GHz Radio Parameters**
- **Configure 6 GHz Radio Parameters**
- **Configure Dual-Band (XOR) Radio Parameters**
- **Configure Tri-Radio Parameters**

Step 7 (Optional) In the **Save As Reusable Template** window, choose one of these options to save the configuration changes as a template, or click **Do Not Save** if you don't want to save the changes at this point:

- To save as a new template, click **Create** and enter a name in the **Template Name** field.

  (Optional) In the **Description** field, enter a description.

- To update the existing template, click **Update**.

  (Optional) In the **Description** field, enter a description.

Step 8 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

Replace a device

This procedure explains how to replace a faulty device.

When replacing a member switch in Cisco switch stacks (hardware stacking), follow the same procedure. The active switch provides the software image and configuration to manage the replacement. Catalyst Center handles the full stack replacement.

Note If you exit the **Replace Device** workflow before completing it, review these guidelines for in-progress cards.

- If a device has an in-progress card on the **Workflows** window and you try to replace the same device from the **Inventory** > **Marked for Replacement** window, a confirmation message with the serial number and task name of **In progress** displays. This message displays because you can start only one **Replace Device** workflow for each device, identified by its serial number. To continue replacing this device, click **Yes**. Otherwise, to start a new workflow for this same device, click **Cancel**, delete the in-progress workflow, and start a new workflow.
- If you click the in-progress card for a device that is unmarked for replacement on the **Workflows** window, a **Warning message** displays. Click **Yes** and choose a different faulty device to start a new workflow. If you click **Cancel**, the workflow is canceled.

Before you begin

- Before marking the device for replacement, import the software image version of the faulty device in the image repository.
- Ensure that the faulty device is unreachable.
- Assign the faulty device to a user-defined site if the replacement device is onboarded to Catalyst Center through Plug and Play (PnP).
- Ensure that the replacement device is not in a provisioning state when you start the **Replace Device** workflow.
- For switch stack replacement, ensure that the faulty and replacement devices have the same number of stack members.
- Ensure the replacement wireless controller is not assigned to any site, not included in High Availability (HA) SSO, and not provisioned.

Procedure

Step 1 From the main menu, choose **Workflows** > **Replace Device**.

Alternatively, you can replace the faulty device from the **Inventory** window. The workflow starts on the **Choose Replacement Device** window (see Step 6, on page 1408). For more information, refer to Replace a faulty device, on page 205.

Step 2 In the **Get started** window, enter a unique task name for your workflow.

Step 3 In the **Choose Device Type** window, choose the type of faulty device that you want to replace.

Step 4 In the **Choose Site** window, choose the site in which you have the faulty device.

Step 5 In the **Choose Faulty Device** window, choose one faulty device that you want to replace.

If you can't find the faulty device, add the faulty device.

a. Click **Add Faulty Device**.

b. Choose the faulty device and click **Next**.

c. In the **Mark for Replacement** window, click **Mark**.

Note In select windows, click **Review** in the bottom-right corner to view the current, summarized configuration details.

Step 6 In the **Choose Replacement Device** window, choose a replacement device from the **Plug and Play** tab or the **Inventory** tab.

The **Plug and Play** tab shows the devices that are onboarded through PnP. The **Inventory** tab shows the devices that are onboarded through inventory or discovery.

For Cisco Catalyst 9800 Series Wireless Controllers and Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in SD-Access fabrics, you can select the **Plug and Play** tab to choose an unclaimed replacement device for zero-touch replacement.

Note If the faulty Cisco Catalyst 9800 Series Wireless Controller or embedded wireless controller is in an IPv6 fabric and runs a version earlier than Cisco IOS XE Release 26.1.1, the **Plug and Play** replacement device option is unavailable. Onboard the replacement device through inventory or discovery, then use the **Replace Device** workflow.

If the replacement device hasn't been onboarded through PnP, add it manually or automatically.

- Manual: Under the **Plug and Play** tab, click **Add Device**. Then in the **Add New Device** window, enter the serial number of the device and click **Add New Device**.
- Automatic: Under the **Plug and Play** tab, click **Sync with Smart Account**. Then, in the **Sync with Smart Account** window, click **Sync**.

Step 7 In the **Configure replacement device** window, provide the required configuration details for replacement.

a) Enter the key in the **Master Encryption Configuration Key** field for the replacement device.

Warning Encrypted passwords and keys cannot be restored without the correct master encryption key.

Step 8 For wireless controllers, in the **Configure replacement device** window, provide the required configuration details for replacement.

a) If the faulty wireless controller has a master encryption key configured, enter the key in the **Master Encryption Configuration Key** field for the replacement wireless controller.

Note Encrypted passwords and keys cannot be restored without the correct master encryption key, which prevents access to the wireless controller and causes the RMA process to fail.

b) Under **Configure HA**, select one of these options:

- **Yes**: for replacing a faulty wireless controller High Availability (HA) pair with a new pair formed using the RMA workflow and two standalone wireless controllers.

  Complete the required configurations for both primary and secondary replacement wireless controllers.

  Note For wireless controllers in a HA pair, use the **Replace Device** workflow only when both devices in the pair are down. This workflow cannot be used to replace a single faulty wireless controller within an active HA pair.

- **No**: for replacing a standalone wireless controller.

  Complete the required configurations for the replacement wireless controller.

To configure a replacement device, you can use the IPv4 address with its corresponding configurations, IPv6 address with its corresponding configurations, or both.

Note The IP address of the faulty wireless controller cannot be reused when claiming the replacement wireless controller through PnP.

Option	Description
Wireless Management IPv4	Enter a valid IPv4 address for the wireless management interface. **Note** • The wireless management IP address of the replacement wireless controller must be different from wireless management IP address of the faulty wireless controller. • To replace a faulty wireless controller HA pair with a new pair, the wireless management IP address of the primary and secondary wireless controllers must be different.
Subnet Mask	Choose a subnet mask for the IPv4 address.
Wireless Management IPv6	Enter a valid IPv6 address for the wireless management interface, if applicable. **Note** • The wireless management IP address of the replacement wireless controller must be different from wireless management IP address of the faulty wireless controller. • To replace a faulty wireless controller HA pair with a new pair, the wireless management IP address of the primary and secondary wireless controllers must be different.
Prefix Length	Choose an IPv6 prefix length.
Gateway IPv4	Enter the default gateway IPv4 address.
Gateway IPv6	Enter the default gateway IPv6 address.
VLAN ID	Enter the VLAN ID. The valid range is from 1 to 4094. **Note** The VLAN ID must be the same for both the faulty and the replacement wireless controller.
Interface Name	Enter the specific interface name used for wireless management.
Local Redundancy Management IP	Enter the local redundancy management IP address for the replacement wireless controller, if applicable. **Note** • Ensure that this IP address and the peer redundancy management IP address are not the same. • Ensure that this IP address is not assigned to any other network entity.

Option	Description
Select Secondary WLC	Choose a secondary wireless controller for HA, if applicable. **Note** To replace a faulty wireless controller HA pair with a new pair: • ensure that the wireless management IP address and subnet mask of the secondary wireless controller are in the same IP subnet as the wireless management IP address of the faulty wireless controller, • ensure that the wireless management VLAN of the secondary wireless controller matches the VLAN of the primary wireless controller, • Future wireless controllers cannot be selected as the primary or secondary wireless controllers. Only unclaimed, onboarded wireless controllers, and unprovisioned inventory-based wireless controllers can be selected.
Peer Redundancy Management IP	Enter the peer redundancy management IP address for the secondary wireless controller, if applicable. **Note** • Ensure that this IP address and the local redundancy management IP address are not the same. • Ensure that this IP address is not assigned to any other network entity.

Step 9 On the **Summary** window, review the summarized details.

If necessary, click **Edit** to update the device type or faulty device details.



Note If Visibility and Control of Configurations is disabled, review the replacement device configuration by clicking **View** under **Replacement Device**.

Step 10 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 11 From the **Inventory** window, view the progress of the device replacement task as the device is replaced.

Alternatively, you can monitor the task from the **Tasks** window.

a. On the **Inventory** window, from the **Focus** drop-down list, choose **Device Replacement**.

b. In the **Replace Status** column, view the replacement status of the device.

   If the device replacement is successful, the **Replaced** status is displayed.

   If the device replacement fails and an error message displays, click the error link. Click **Retry** to retry the workflow with the same set of faulty and replacement devices.



Note The main inventory window displays the details of the new replacement device that has replaced the faulty device.

c. In the **Replace Status** column, click the status of the device to view more information in a slide-in pane.

   For example, the slide-in pane displays these steps that the system follows to complete the task:

   1. Run readiness checks for device replacement.
   2. Claim the (PnP) replacement device.
   3. Distribute and activate the software image to the replacement device.
   4. Deploy licenses.
   5. Provision VLAN configurations.
   6. Provision startup configurations.
   7. Reload the replacement device.
   8. Check for reachability of the replacement device.
   9. Deploy SNMPv3 credentials to the replacement device.
   10. Synchronize the replacement device.
   11. Remove the faulty device from CSSM.
   12. Add the replacement device to CSSM.
   13. Revoke and create the PKI certificate.
   14. Update Cisco ISE.
   15. Delete the faulty device.

What to do next

During wireless controller replacement, these files and configurations are not transferred to the replacement wireless controller:

- Custom web authentication bundles and NBAR protocol packs
- IP address SSH RSA keys or key pair names

- Custom trust points
- Regulatory activation file

After replacement, copy and reconfigure these settings manually on the replacement wireless controller.

Switch refresh

Switch Refresh workflow allows you to replace an older switch that has reached its End of Life (EoX), with a new switch. For example, a Cisco Catalyst 3650 Switch can be replaced by a Cisco Catalyst 9300 Switch.



Note Currently switch refresh is available for Cisco Catalyst 3650 and Cisco Catalyst 3850 Switches running on Cisco IOS XE.

The feature has these limitations:

- Unsupported Operating System: The old devices (Cisco Catalyst 2000, 3000, 4000, 6000 Series Switches) running on Cisco IOS images are not supported. Only old devices running on Cisco IOS XE (Cisco Catalyst 3650 and 3850 Series Switches) are supported.
- Inconsistent port type or speed: New devices having different port types or speeds compared to the older devices are not supported. For example, Gigabit Ethernet to 10-Gigabit Ethernet is not supported.
- Minimum software version requirement for a new device: For Cisco Catalyst 3650 Series, 3850 Series, and 9300 Series switches, the minimum required software version is 16.9.x.
- Plug and Play (PnP) onboarding in Fabric networks: PnP onboarding for the new devices in a fabric network is not supported. To onboard new device through PnP, you must manually set the IP address and PnP profile on the new device.

Before you begin

Make sure that these conditions are met:

- Port count: The new device can have the same number of ports or more ports than the older device.

  For example, a 24-port Cisco Catalyst 3650 Switch can be replaced with a 24-port Cisco Catalyst 9300 Switch or a 48-port Cisco Catalyst 9300 Switch.
- Port type: The port type must be the same for old and new device.
- Device reachability: Ensure that the older device is in unreachable state before proceeding with the workflow.
- Stack member count: For a stacked switch, the switch member count should be same or more in the new device.
- Role consistency: The devices that are selected in a workflow should be of the same role.
- Port connection: Ensure that all ports on the new device are connected in the same manner as the old device.

Procedure

Step 1 From the main menu, choose **Provision** > **Inventory**.

Step 2 Check the check box next to the older device that you want to replace and choose **Actions** > **Switch Refresh** > **Mark for Refresh**.

Step 3 In the confirmation window, click **Mark**.

A **Success** message displays and the older device is successfully marked for replacement.

Step 4 Choose the older device or devices, and then choose **Actions** > **Device Refresh** > **Refresh Device(s)**.

The Switch Refresh workflow is triggered.

Alternatively, to trigger the workflow, choose **Workflows** > **Switch Refresh**.

Step 5 If a task overview window displays, click **Let's Do It** to go directly to the workflow.

Step 6 In the **Task Name** field, enter a unique name and click **Next**.

Step 7 In the **Pre-requisites** window, if a golden image is already tagged to the new device, click **Next**. Otherwise, click **Image Repository** hyperlink to tag a golden image to the new device.

For information on how to tag a golden image, see Mark a software image as standard, on page 545.

After completing the task, go to the **Switch Refresh** workflow tab, and click **Next**.

Note If the older switch is configured with MD5 and the newer switch's golden image is later than 17.14.1, the newer switch will be configured with SHA.

Step 8 In the **Select Devices** window, choose the older device that was marked for replacement and click **Next**.

Step 9 In the **Replace old device with the new device** window, do these steps:

a. If required, edit the default **New Device Name**.

b. Choose the device **Platform** and **Serial Number** from the drop-down list.

c. Click **Next**.

Step 10 In the **Resolve Dependencies** window, if the device is not assigned a golden image, you cannot proceed with the workflow.

a) To assign a golden image to the device, click **Image Repository** hyperlink and follow the procedure that is mentioned in Mark a software image as standard, on page 545.

b) Enter the required **Master encryption configuration key** for each device. Verify the "Entered" status for the key, and click **Next**

Step 11 In the **View Device Configuration** window, review the configuration that will be pushed to the new device from the older device and click **Next**.

Step 12 In the **Schedule Task** window, click **Now** to start device replacement immediately or click **Later** to schedule the device replacement at a specific time. Click **Next**.

Step 13 In the **Summary** window, review the configuration settings and click **Refresh Devices**.

The replacement of the older device with the new device is initiated.

Step 14 Click **Monitor Refresh Status** to view the replacement device status.

The **Inventory** window displays. You can view the device replacement status under the **Refresh Status** column.

Step 15 Click the link under the **Refresh Status** column to view the ongoing process.

Step 16 Click **Refresh**. This process might take some time.

Upon successful device replacement, the older device is replaced with the new device.

Create a remote support authorization

Use this procedure to create a remote support authorization.

Note The Catalyst Center remote support authorization is supported only with RADKit version 1.2.1 and later.

Procedure

Step 1 From the main menu, choose **Workflows** > **Create a Remote Support Authorization**.

Step 2 If a task overview window is displayed, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Access Permission Agreement** window, do these steps:

a) Check the **I agree to provide access to network devices** check box to provide access to network devices.

b) Check the **I agree to provide access to Catalyst Center** check box to allow a Cisco specialist to access your Catalyst Center setup using SSH credentials.

Note You can revoke the authorization at any time before it expires. To revoke the authorization, see View the Remote Support Authorization Dashboard.

Step 4 Click **Next Step**.

Step 5 In the **Set up the Authorization** window, complete these fields:

- **Cisco Specialist Email Address**
- **Access Role for the Cisco Specialist**
- **Existing Case Number(s)**
- **Access Justification**

Step 6 Click **Next Step**.

Step 7 In the **Schedule the Access** window, click **Now** or **Later** to indicate when you want to allow the Cisco specialist to access Catalyst Center.

Step 8 Click **Next Step**.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Create**.

The **Done! Authorization is created** window displays.

Step 11 Click **View All Authorizations** to navigate to the **Remote Support Authorization** window. For information, see View the Remote Support Authorization Dashboard.

Create an event notification

Catalyst Center event notification allows you to associate multiple channels inside one notification that delivers the details of selected events that occur at multiple points.

Procedure

Step 1 From the main menu, choose **Workflows** > **Create a New Notification**.

Step 2 If a task overview window opens, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Select Channels** window, select the notification channels.

The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, **EMAIL**, and custom channels. Assurance events do not support SNMP.

Step 4 In the **Select Site and Events** window, from the **Select a site** drop-down list, select a specific site for which you want to be notified for the selected events.

Note You can select multiple sites at a time.

Step 5 Click either the plus icon next to an event, or click **Add All** to add all the events to the respective notification.

Step 6 To remove an event from the notification, click either the cross icon next to the event that you want to remove, or click **Remove All** to remove all the event from the event list.

Note

- When you select a notification channel, a table in the **Select Site and Events** window lists the number of events supported by the chosen notification channel.
- When you select more than one notification channel, a table in the **Select Site and Events** window lists the number of supported events that are common in the chosen notification channels.

Step 7 In the **Configure Notification** window, configure these values:

a. If you select an **EMAIL** notification channel, configure these in the **Email Settings** window:

1. Click the link to access the **Email GUI** window and configure a new email server.



Note

- Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **EMAIL**, but have not yet configured the email settings, you are prompted to access the **GUI** window where you can perform this task. Email settings are configured in the **Email** tab.

  (Optional) To access the **Email** tab, click the menu icon and choose **System** > **Settings** > **External Services**.

  Expand **External Services**, select **Destinations**, and click the **Email** tab.

- Up to 20 email addresses per endpoint can be configured to receive email notifications. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center validates the email addresses and notifies you if the syntax is incorrect.
- If you need to configure more than 20 email addresses per endpoint, you can use a group email alias.
- When using email destinations for event subscriptions, the emails that are sent show events with a UTC timestamp.

2. Click either **Select Existing Instance** to use the existing email instance or **Create New Instance** to create a new email instance.

3. If you click **Select Existing Instance**, from the **Select Instance** drop-down list, select an email instance.

4. Enter the email addresses in the **From** and **To** fields and a subject for the **Subject** header in the email.

b. If you select a **SYSLOG** notification, configure these values in the **Syslog Settings** window:

1. Click the link to access the **Syslog** GUI window and configure a new syslog endpoint (syslog server hostname and port number).



Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **SYSLOG**, but have not yet configured the syslog server settings, you are prompted to access the GUI window where you can perform this task. Syslog server settings are configured in the **Syslog** tab.

(Optional) To access the **Syslog** tab, click the menu icon and choose **System** > **Settings** > **External Services**.

Expand **External Services**, select **Destinations**, and click the **Syslog** tab.

2. In the **Protocol** field, enter either TCP or UDP.

3. In the **Port** field, enter the port number of the syslog server.

4. In the **Hostname/IP** field, enter the hostname or IP address of the syslog server.

5. From the **Select Instance** drop-down list, select the syslog instance.

c. If you select a **REST** notification, configure these values in the **REST Settings** window:

- Click the link to access the **REST Webhook** GUI window and configure a new webhook endpoint.



Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **REST**, but have not yet configured the webhook settings, you are prompted to access the GUI window where you can perform this task. Webhook settings are configured in the **Webhook** tab.

(Optional) To access the **Webhook** tab, click the menu icon and choose **System** > **Settings** > **External Services**.

Expand **External Services**, select **Destinations**, and click the **Webhook** tab.

- From the **Webhook Instance** drop-down list, select a notification endpoint and URL.
- In the **URL** field, enter the URL address of the REST API endpoint that the event will be sent to.

  Trust certificate: Whether a trust certificate is required for REST API endpoint notification.

  Method: Either the PUT or POST method.

- **Basic**: Authentication where the client sends HTTP requests with the word *Basic* in the authorization header, followed by a space and a base64-encoded string username:password. If you select **Basic** in the GUI, the **Headers** field is automatically populated with the **Authorization** value.
- **Token**: Authentication where users are authenticated using a security token provided by the server. If you select **Token**, the **Headers** field is automatically populated with the **X-Auth-Token** value.
- **No Authentication**: No authentication needed.
- **Headers**: The **Header Name** and **Header Value**.



Note The **Headers** fields may be automatically populated depending on your Authentication selection.

d. If you select **SNMP** notification channel, configure these values in the **SNMP Settings** window:

1. Click the link to access the **SNMP** GUI window and configure a new SNMP endpoint.

Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **SNMP**, but have not yet configured the SNMP settings, you are prompted to access the GUI window where you can do this task. SNMP settings are configured in the **SNMP** tab.

(Optional) To access the **SNMP** tab, click the menu icon and choose **System** > **Settings** > **External Services**.

Expand **External Services**, select **Destinations**, and click the **SNMP** tab.

The SNMP trap notification is only available for a system hardware event. When the health state of hardware components changes, a system hardware event triggers notifications to subscribers. Hardware components monitored for changes include CPU, memory, disk, NIC, fan, power supply, and RAID controller.

2. From the **SNMP Instance** drop-down list, select the notification endpoint.
3. **Create a new endpoint**: Enter a new endpoint name and description.
4. In the **Hostname/IP Address** field, enter the hostname or IP address for the SNMP trap receiver (server).
5. In the **Port** field, enter the port number for the SNMP trap receiver (server).

e. If you select **PAGERDUTY** notification channel, configure it in the **PAGERDUTY settings** window:

1. In the **SERVICE CONFIGURATION** area, click either **Select Existing Instance** to use the existing PagerDuty instance or **Create New Instance** to create a new PagerDuty instance.
2. From the **Select Instance** drop-down list, select a PagerDuty instance.
3. In the **PagerDuty Events API URL** field, enter a PagerDuty event API URL.
4. In the **PagerDuty Integration Key** field, enter a PagerDuty integration key.

f. If you select **WEBEX** notification channel, configure these values in the **WEBEX Settings** window:

1. From the **Select Instance** drop-down list, select a Webex instance.
2. In the **Webex URL** field, enter the Webex URL.
3. In the **Webex Room ID** field, enter the Webex room ID.
4. In the **Webex Bot Access Token** field, enter the Webex bot access token.

Step 8 Click **Save**.

In the **Name and Description** window, do these steps:

a) In the **Name** field, enter a unique name for the notification.
b) In the **Description** box, enter a description of the notification.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Finish**.

The **Done! Your new notification is complete** window appears.

Configure Remote LAN

Remote LAN (RLAN) allows you to configure RLAN ports on APs for Cisco Wireless Controller. A wireless controller authenticates the wired clients and allows them to connect to the network.

Catalyst Center supports RLAN configuration only on Cisco Catalyst 9800 Series Wireless Controller. You can configure RLAN for nonfabric sites on wireless controllers that run Cisco IOS XE Release 16.12 or later. You can configure RLAN for fabric sites on wireless controllers that run Cisco IOS XE Release 17.7 or later.

Any changes in the network settings or network profile (for example, AP profile, RF profile, site tags, and so on) are pushed as part of the RLAN workflow and may result in network disruption for the connected clients.

Note Catalyst Center doesn't support RLAN configuration on Cisco AireOS Wireless Controllers.

Use this procedure to configure RLAN ports.

Before you begin

- Ensure that you have provisioned a wireless controller and at least one AP for the sites where you want to configure the RLAN ports.
- Any change in CLI templates and feature templates in the associated network profiles aren't configured in this workflow. Ensure that the provision status of the associated wireless controller is up to date on the **Inventory** window. If there's an **Out of Sync** notification next to the provision status, reprovision the wireless controller before configuring RLAN.

To configure RLAN ports for fabric sites:

- Ensure that you have provisioned the required fabric site.
- Ensure that you have created IP pools and Security Group Tags (SGT).

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure RLAN**.

Step 2 If a task overview window displays, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Get Started** window, enter a unique name for the task.

Step 4 In the **Select Sites** window, select the sites where you want to configure RLAN ports.

Note You can select multiple sites, but the selected sites must be managed by the same Cisco Catalyst 9800 Series Wireless Controller.

Assigning the RLAN configuration to APs on the selected sites can potentially impact the RLAN configuration for APs on the other sites based on the policy tag assignment.

The right pane shows the summary of the selected sites. Catalyst Center configures RLAN for all the APs provisioned on the floors of the selected sites.

Step 5 In the **Select Policy Tags** window, check the check box next to the policy tags for which you want to configure RLAN.

This selection can potentially impact the RLAN configuration for APs on the other sites based on the policy tag assignment.

- To view the impacted sites for a policy tag, click the corresponding number under **Impacted Sites**. In the **Impacted Sites** dialog box, to search for a site, in the **Search Table** field, enter either the partial name or full name of the site and press **Enter**.
- To view the impacted APs for a policy tag, click the corresponding number under **Impacted APs**. In the **Impacted Access Points** dialog box, to filter APs based on specific details, click the search icon and select from the filter options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Select the required option in the filter and click **Apply**.

Step 6 In the **Remote LAN Configuration** window, do these steps:

a) Select the required RLAN port from the **Port 1**, **Port 2**, and **Port 3** options.

Sites can have APs with different number of LAN ports. RLAN configuration is applied to the corresponding LAN port number. If an AP has a single RLAN port, Catalyst Center ignores the **Port 2** and **Port 3** configurations for the AP.

When a site is managed by a secondary wireless controller, the VLANs configured for the RLAN client on the secondary wireless controller are the same as the VLANs configured on the primary wireless controller.

b) To enable or disable RLAN for the corresponding port, use the **AP LAN Port** toggle button.

c) To configure RLAN ports for a fabric site, use the **Fabric** toggle button.

This toggle is available only if the device is in a fabric site. If you enable the **Fabric** toggle button, do these tasks:

- In the **IP Address Pool** field, enter the IP address.
- (Optional) From the **Scalable Group Tag** drop-down list, select the required option.

d) (Optional) In the **RLAN Profile** tab, from the **RLAN Profile** drop-down list, select an RLAN profile.

To create an RLAN profile, click **Create New** and do these steps:

1. In the **RLAN Profile Name** field of the **Create new RLAN Profile** dialog box, enter a name for the RLAN profile.

   If there's an existing RLAN profile, to copy the configurations from it, check the **Copy Configuration from Existing RLAN Profile** check box. From the **RLAN Profile** drop-down list, select an existing RLAN profile.

2. Click **Save**.

If you select an RLAN profile, do these tasks:

- To enable or disable the RLAN profile, use the **Admin Status** toggle button.
- In the **Maximum End Points** field, enter the number of endpoints. The valid range is from 0 through 10000.



Note This field configures the client connections per RLAN. 0 indicates unlimited client connections.

- (Optional) From the **Layer 2** drop-down list, select the required option: **Dot1x** or **Open**
- (Optional) From the **Layer 3** drop-down list, select the required option: **Open** or **Internal Web Authentication**
- (Optional) From the **Select a AAA Server Group** drop-down list, select an AAA server group.

  This drop-down lists the AAA server groups configured as part of WLAN provisioning on the primary controller. If you don't select an AAA server group, Catalyst Center configures the default method under the RLAN profile for the selected security settings.

Note This drop-down list is available only when the Layer 2 is **Dot1x** or Layer 3 is **Internal Web Authentication**.

- (Optional) To enable MAC filtering, check the **MAC Filtering** check box.
- (Optional) From the **Fallback Authentication** drop-down list, select the required fallback authentication: **None**, **Dot1x on MAC Filtering Failure**, or **MAC Filtering on Dot1x Failure**.

Note Fallback authentication is available only if Layer 2 is **Dot1x** and MAC filtering is enabled.

e) (Optional) Click the **RLAN Policy** tab, from the **RLAN Policy** drop-down list, select an RLAN policy.

To create an RLAN policy, click **Create New** and do these steps:

1. In the **RLAN Policy Name** field of the **Create new RLAN Policy** dialog box, enter a name for the RLAN policy.

   If there's an existing RLAN policy, to copy the configurations from it, check the **Copy Configuration from Existing RLAN Policy** check box. From the **RLAN Policy** drop-down list, select an existing RLAN policy.
2. Click **Save**.

If you select an RLAN policy, do these tasks:

- To enable or disable the RLAN policy, use the **Admin Status** toggle button.
- From the **Forwarding Mode** drop-down list, select the required option: **Local Switching** or **Central Switching**

  If you select local switching, in the **VLAN** field, enter the VLAN name. If you select central switching, in the **VLAN ID** field, enter the VLAN ID. The valid range for VLAN ID is from 1 through 4096.

Note
- The Cisco Aironet 1815T Access Point doesn't support local switching for RLAN. For other AP models, when the AP is in local mode, local switching for RLAN is supported for Cisco IOS XE Release 17.2 or later.
- If you enable the **Fabric** toggle button, the **Central Switching** option isn't available.

- In the **Timeout Period (in seconds)** field, enter the timeout period, in seconds. The valid range for timeout is from 0 through 86400.
- To enable or disable Point over Ethernet (PoE), use the **PoE** toggle button.

Note Catalyst Center enables PoE only on APs with PoE-capable ports.

- (Optional) To enable AAA override, check the **AAA override** check box.

f) In the **Review Impacted Sites** dialog box, review the details about the impacted sites and click **Confirm**.

Step 7 (Optional) In the **Delete Unused RLAN Profiles and Policies** window, check the next to the unused RLAN profiles and RLAN policies that you want to delete.

This window lists the unused RLAN profiles and RLAN policies on the selected wireless controller. Deleting them optimizes the wireless controller storage.

Step 8 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 9 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 10 On the **Tasks** window, monitor the task deployment.

What to do next

You can view the status of the RLAN configuration in the **Activities** > **Tasks** window.

If you have provisioned a secondary wireless controller, reprovision the secondary wireless controller from the **Provision** > **Inventory** window.

Configure Parallel Redundancy Protocol in a fabric site

This workflow helps you set up Parallel Redundancy Protocol (PRP) channels, which are used to ensure high availability and zero packet loss in critical network systems. PRP configuration is compatible with Cisco Catalyst IE3400 and IE3400H Rugged Series switches that run Cisco IOS XE Release 17.16.x or later.

Note Catalyst Center does not support PRP configuration on FIAB.

Before you begin

- Ensure RedBox is not connected to LAN-B edge device. This may cause loop in the network resulting in network congestion.
- Ensure any existing PRP configuration is cleared in the LAN-B edge device.

Procedure

Step 1 From the main menu, choose **Workflows** > **Configure PRP**.

Alternatively, you can navigate to the fabric site topology view, choose the extended node on which you want to configure PRP and click **Enable PRP** under the **PRP** tab.

Step 2 If a task overview window displays, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Select a site** window, choose a fabric site associated with the RedBox on which you want to configure PRP.

Step 4 In the **Select a RedBox device** window, choose a RedBox device.

Step 5 In the **Configure PRP Channel** window, choose the interface pair that act as primary and secondary interfaces for this switch to enable redundancy.

Step 6 In the **Enable Precision Time Protocol** window, click **Next**.

Precision Time Protocol (PTP) is not configurable at this moment.

Step 7 In the **Configure VLAN** window, complete the switchport and VLAN settings.

- **Switchport mode**: Choose **Trunk mode**.
- **Allowed VLANs**: Click **All** or **List** radio button. If you choose **List** option, enter the VLANs in the **Allowed VLANs** field.
- **Supervisory frame tagging**: Click the **Tag Supervisory frames** toggle button and configure the tagging type.
  - **Single VLAN**: Enter the **VLAN ID**.
  - **VLAN aware**: Enter the VLANs and click the **Reject untagged supervisory frame** toggle button to enhance network security and segmentation.

Step 8 In the **Configure LAN** window, complete the LAN-B settings.

- **LAN-B site**: Choose a fabric site.
- **LAN-B switch**: Choose a switch from the listed edge nodes to use as your LAN-B device.
- **LAN-B interface**: Choose an interface to use on the selected LAN-B switch.

  The drop-down list shows the interfaces that are available for PRP configuration including administratively down ports. The ports participating in port channel or PRP channel are not shown in the drop-down list.

Step 9 In the **Summary** window, review and confirm the PRP configuration.

Step 10 Click **Deploy**.

Step 11 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200.

Step 12 On the **Tasks** window, monitor the task deployment.

What to do next

Connect the RedBox interface to the correct LAN-B interface.

Delete PRP configuration

If you want to modify the PRP configuration, you must delete the PRP configuration from the LAN-A edge device and LAN-B edge device and redo the PRP configuration.

Before you begin

You must remove the device configured as RedBox from fabric site and delete the device from inventory. For more information, see Remove a device from a fabric, on page 1025 and Delete a network device, on page 183.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Click the fabric site from which you want to delete the PRP configuration.

Step 4 In the **Port Assignment** tab, choose the PRP LAN-A or PRP LAN-B port from which you want to delete the PRP configuration.

Step 5 Hover your cursor over **More Actions**, and click **Delete PRP**.

Step 6 Follow the onscreen guidelines to delete the PRP configuration.

Step 7 Click **Deploy**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200

Step 9 On the **Tasks** window, monitor the task deployment.

Edit PRP channel

Modify the Allowed VLAN details in the PRP configuration.

Procedure

Step 1 From the main menu, choose **Provision** > **Fabric Sites**.

Step 2 Click the fabric site where you want to edit the PRP channel.

Step 3 Click the **Port Assignment** tab and choose the device configured as RedBox.

Step 4 Hover over **More Actions**, then, click **Edit PRP Channel**.

Alternatively, click the **PRP-channel** under **Interface** column.

Step 5 In the **Edit PRP Channel** slide-in pane, edit the Allowed VLAN details as required. Click **Update.**

Step 6 Follow the onscreen guidelines to edit the PRP channel configuration.

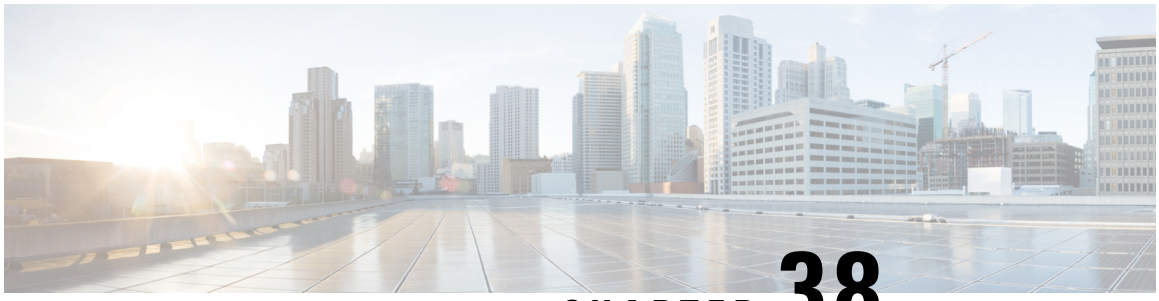
Step 7 Click **Deploy**.

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later, on page 199.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations, on page 200

Step 9 On the **Tasks** window, monitor the task deployment.



CHAPTER 38

Wireless Network Configuration Use Cases

- Wireless network configuration use case, on page 1427
- Wireless controller management use cases, on page 1427
- Wi-Fi 7 configuration use case, on page 1430
- High availability use cases, on page 1432
- Wireless mobility use cases, on page 1435
- AP management use cases, on page 1441
- Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers, on page 1450

Wireless network configuration use case

Use these use cases to learn about wireless network configuration.

For information about optimal network management using wireless automation, see *Leveraging Cisco Catalyst Center Wireless Automation for Optimal Network Management*.

Wireless controller management use cases

These topics help you understand the wireless controller management use cases for wireless networks.

WLAN profile and policy profile configuration

Catalyst Center provides flexibility and intelligence when managing SSIDs across complex site hierarchies. Catalyst Center dynamically selects the WLAN profile and policy profile names from either network settings or network profiles based on the design intent and the specific site context.

SSID defined at Global site without override

When an SSID is defined at the Global site without any overrides at the site hierarchy, the WLAN profile and policy profile names are based on the network profile for that site.

Catalyst Center automatically detects conflicts when the same SSID is associated with the same WLAN profile and policy profile names but configured with different configuration flavors across multiple network profiles. For example, the SSID `store_wifi` with WLAN profile and policy profile name `store_wifi_area1` is defined

as Flex in the network profile attached to `Site1` and non-Flex in the network profile attached to `Site2`. If `Site1` and `Site2` are managed by the same wireless controller, it is a conflicting configuration.

To resolve conflicts, update each network profile to have unique WLAN profile and policy profile names. For example, update the network profile for `Site2` with the WLAN profile and policy profile name as `store_wifi_area1_site2`.

SSID overridden at child sites

When an SSID is overridden at child sites, Catalyst Center determines the WLAN profile and policy profile names based on either the network setting or network profile, based on these conditions:

Profile name selection	Criteria
From network settings	• WLAN profile and policy profile names in the network profile are the same as the names in the Global network settings. • The same WLAN profile or policy profile name is used across all network profiles under the overridden site.
From network profile	Multiple network profiles exist, each with a unique WLAN profile and policy profile name.

Catalyst Center automatically detects conflicts when the same SSID and WLAN profile or policy profile names are used with different configurations in two or more network profiles.

For example, a wireless controller manages a network with the SSID `store_wifi` and this hierarchy:

- Area1
  - Site1 (`store_wifi_area1`)
    - Building-01
      - Floor1
      - Floor2
  - Site2 (`store_wifi_area1`)
    - Building-02
      - Floor1
      - Floor2

This table lists the conflict configuration examples and resolutions.

Example	Resolution
The WLAN profile or policy profile name is `store_wifi_profile`. The SSID is defined as: • Flex configuration in `Site1` associated with `Network Profile-1` • Nonflex configuration in `Site2` associated with `Network Profile-2` The wireless controller detects a conflict as it manages both the sites.	Update each network profile to use a unique WLAN or policy profile name (for example, `store_wifi_area1_site2` for `Site2`).
The wireless controller manages only the buildings from the hierarchy using two network profiles, one for each floor. • `Network Profile-1` for first floors in each building using WLAN profile and policy profile name `store_wifi_area1_np1`. • `Network Profile-2` for second floors in each building using WLAN profile and policy profile name `store_wifi_area1_np2`. Overrides are configured at two sites but with same WLAN profile and policy profile name `store_wifi_area1`. Catalyst Center finds granular-level profile names at `Network Profile-1` and `Network Profile-2` under each overridden site (`Site1` and `Site2`). The wireless controller detects a conflict as the SSID is overridden at `Site1` and `Site2` with different configurations using the same WLAN profile and policy profile name `store_wifi_area1_np1`.	• Use a single network profile for all managed floors if there are no configuration differences at the network profile level. • Apply common configuration at the area-level network settings. • Create a network profile for each floor with unique WLAN profile and policy profile names.

WLAN profile or policy profile name modification

Catalyst Center automatically detects the migrated SSIDs when the wireless controller is reprovisioned without any intent change. Catalyst Center reuses the WLAN profile and policy profile name based on these conditions:

- The site level override is same as before migration.
- The WLAN profile or policy profile name is same as before migration in either the network profile or network settings.

These conditions are also applicable to non-migrated SSIDs which are created in Release 2.3.7.7 and reprovisioned with a WLAN profile or policy profile name change.

If you change the WLAN profile or policy profile name of an SSID at either the site hierarchy (**Network Settings** > **Wireless** > **SSID**) or the network profile and then reprovision the wireless controller, Catalyst Center tries to reuse the provisioned WLAN profile or policy profile names for a site if the SSID is already provisioned to the wireless controller for the same site with a WLAN profile or policy profile name that matches either the WLAN profile or policy profile name defined in the network profile or network settings. Catalyst Center ignores the updated profile name and continues to use the existing profile name.

For example, a wireless controller manages a network with the SSID `store_wifi` created at the Global level using WLAN profile or policy profile name `store_wifi_profile`. The network hierarchy under Global is:

- Area1
  - Site1

- Building-01
  - Floor1
  - Floor2
- Site2
  - Building-02
    - Floor1
    - Floor2

- Example 1:
  - The network profile `Network Profile-1` is assigned to all floors of `Site1/Building-01` with the WLAN profile or policy profile name `store_wifi_area1_np1`.
  - The network profile `Network Profile-2` is assigned to all floors of `Site2/Building-02` with the WLAN profile or policy profile name `store_wifi_area1_np2`.

  When you provision the wireless controller, the WLAN profile and policy profiles `store_wifi_area1_np1` and `store_wifi_area1_np2` are created on the wireless controller.

  To use a new WLAN profile or policy profile name (for example, `store_wifi_area1_np1_1`) for the sites using `Network Profile-1`, you can update the profile name in `Network Profile-1` and then reprovision the wireless controller. The new profile name is used. Similarly, if you change the profile name in `Network Profile-2` to `store_wifi_area1_np2_1` and reprovision the wireless controller, it uses the updated profile name.
- Example 2: A single network profile `Network Profile-1` with `store_wifi_profile` as the WLAN profile and policy profile names is used for all the floors.

  When you provision the wireless controller managing all the floors, the WLAN profile and policy profile `store_wifi_profile` is applied to all the floors.

  To update the WLAN profile or policy profile name used by the wireless controller, you must update the name in `Network Profile-1` and the SSID configuration in global network settings to ensure that the new profile name is correctly applied.

Wi-Fi 7 configuration use case

This section helps you understand the Wi-Fi 7 configuration use case for wireless networks.

Enable the Wi-Fi 7 configuration

Use this procedure to enable the Wi-Fi 7 configuration on Catalyst Center.

Before you begin

- Ensure that the Wi-Fi 7 APs are available in the **Provision** > **Inventory** window.

The Wi-Fi 7 APs include:

- Cisco Wireless 9171I Series Access Points running Cisco IOS XE Release 17.18 or later,
- Cisco Catalyst 9172H Series Access Points,
- Cisco Catalyst 9172I Series Access Points,
- Cisco Catalyst 9176D1 Series Access Points running Cisco IOS XE Release 17.17.1 or later,
- Cisco Catalyst 9176I Series Access Points running Cisco IOS XE Release 17.17.1 or later, and
- Cisco Wireless 9177D Series Access Points
- Cisco Wireless 9177E Series Access Points
- Cisco Wireless 9177I Series Access Points
- Cisco Catalyst 9178I Series Access Points.

- The devices must be running Cisco IOS XE Release 17.15.2 or later.
- Wi-Fi 7 APs use CNS licenses. If these APs don't meet the license requirements, they operate in worldwide safe mode (WWSM).

  To disable WWSM and meet the license requirements, enable the CNS licenses in the **License Manager** window. For more information, see "Manage Licenses" in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 Enable the 802.11be status for the 2.4-GHz, 5-GHz, and 6-GHz radio bands in the **Dot11be Status Configuration** feature template.

You can use the existing default profiles or create custom profiles for each radio band. For more information, see Create a feature template for Dot 11be status configuration, on page 521.

Step 2 Create an RF profile with the necessary settings and configure the required Wi-Fi 7 settings.

- Enable preamble puncturing using the **Preamble Puncturing** toggle button for the 5-GHz and 6-GHz radio bands.
- Use the **DBS Channel Width** slider to set the maximum channel width of 320 MHz for the 6-GHz radio band.
- Check the corresponding check box to enable the 802.11be parameters for the 6-GHz radio band.
  - Downlink OFDMA
  - Uplink OFDMA
  - Downlink MU-MIMO
  - Uplink MU-MIMO
  - OFDMA Multi-RU

Note Starting with Cisco IOS XE Release 17.18.2, the OFDMA uplink, OFDMA downlink, MU-MIMO uplink, and MU-MIMO downlink configurations are deprecated and ignored under the **802.11BE PARAMETERS**. To configure these settings, use the **802.11AX PARAMETERS** section.

For more information, see Create a wireless radio frequency profile, on page 383.

Step 3 Create a 802.11be profile.

- Configure the 802.11be settings for the 2.4-GHz and 5-GHz radio bands.

Note This 802.11be profile is mapped to the WLAN and applies to only the 2.4-GHz and 5-GHz radio bands. The 802.11be configuration for the 6-GHz radio band is used from the corresponding settings in the RF profile.

- Configure the MLO group settings for all radio bands.

For more information, see Create an 802.11be profile, on page 446.

Step 4 In the associated wireless network profile,

- Associate the 802.11be profile with the corresponding SSID in the network profile (for more information, see Add SSIDs to a network profile, on page 460) and
- Add the **Dot11be Status Configuration** feature template to the network profile (for more information, see Add feature templates to a network profile, on page 464).

Step 5 (Optional) In the corresponding SSID, check the **AP Beacon Protection** check box to enable AP beacon protection.

For more information, see Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

Step 6 Configure the Wi-Fi 7 APs.

For more information, see Configure APs, on page 1382.

Step 7 Provision the Wi-Fi 7 APs with the associated network profile.

For more information, see Provision Cisco APs on day 1, on page 627.

High availability use cases

These topics help you understand the high availability (HA) use cases for wireless networks.

Configure Cisco Wireless Controller HA

Cisco Wireless Controller HA allows you to use a wireless controller as a backup for a primary wireless controller. The active wireless controller handles all the APs, client traffic, and shares the AP and client database with the standby wireless controller. If there is a failover, the standby wireless controller takes over immediately, resulting in zero client service downtime and zero SSID outage.

Before you begin

- Ensure that both the wireless controllers are of the same form factors.
- Ensure that both the wireless controllers are running the same software version.
- Wireless controller HA supports a maximum redundancy port link latency of 80 ms round-trip time (RTT), minimum bandwidth of 60 Mbps, and minimum maximum transmission unit (MTU) of 1500.
- Ensure that you connect the redundancy ports of both the wireless controllers physically or through a Layer 2 virtual network. If you connect redundancy ports through a Layer 2 virtual network, ensure that the link latency, bandwidth, and MTU requirements are met.
- For the Cisco Catalyst 9800-CL Wireless Controllers running on ESXi, KVM, and Hyper-V, ensure that the redundancy port connects to the same vswitch.

Procedure

Step 1 Ensure that you have the wireless controller in your inventory. For more information, see About Inventory, on page 78 and Add a network device, on page 130.

If the wireless controller isn't available in the inventory, use the Discovery feature to discover it. For more information, see Discover Your Network, on page 55.

Step 2 Ensure that both the wireless controllers are in the **Managed** state in the inventory. For more information, see Display information about your inventory, on page 80.

Step 3 Use the **show redundancy** command to verify that the operating redundancy mode is **Non-redundant** on both the wireless controllers.

Step 4 From the main menu, choose **Provision** > **Inventory**.

Step 5 Check the check box next to the required wireless controller, and then click **Actions** > **Provision** > **Configure WLC HA**.

Step 6 Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** addresses.

You must configure the IP addresses used for redundancy management IP and peer redundancy management IP in the same subnet as the management interface of the wireless controller. Ensure that these IP addresses are unused IP addresses within that subnet range.

Step 7 Enter the **Netmask**.

Step 8 From the **Select Secondary WLC** drop-down list, choose the secondary wireless controller.

Step 9 Since the Cisco Catalyst 9800-CL Wireless Controller doesn't have a dedicated redundancy port, choose the interface that will be used for the redundancy port.

Note Appliance-based Cisco Catalyst 9800 Series Wireless Controllers have dedicated redundancy ports, and redundancy port interface selection isn't necessary for these devices.

Step 10 Click **Configure HA**.

What to do next

To verify the status of HA, use the **show redundancy** command. This is a sample output of the command:

```
  cat_9800-1 #show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 5 minutes
Switchovers system experienced = 0
              Standby failures = 0
       Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
------------------------------
              Active Location = slot 1
       Current Software state = ACTIVE
      Uptime in current state = 5 minutes
                Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
        Configuration register = 0x2102
                Recovery mode  = Not Applicable

Peer Processor Information :
---------------------------
              Standby Location = slot 2
       Current Software state = STANDBY HOT
      Uptime in current state = 3 minutes
                Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
                      BOOT =
                 CONFIG_FILE =
        Configuration register = 0x2102
```

To verify the **Priority** of the primary wireless controller, use the **show chassis** command. The **Priority** of the primary wireless controller is changed to 2 to ensure that its role is **Active**. This is a sample output of the command:

```
  cat_9800-1 #show chassis
Chassis/Stack Mac Address : 000c.2972.9b46 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
-----------------------------------------------------------------------------------
*1       Active   000c.2972.9b46     2      V02     Ready               172.16.0.2
 2       Standby  0050.56ae.a54f     1      V02     Ready               172.16.0.3
```

Configure Cisco Wireless Controller N+1 HA

Cisco Wireless Controller N+1 HA allows you to use a wireless controller as a backup for multiple primary wireless controllers. Catalyst Center doesn't support stateful switchover for N+1 HA and each wireless controller must be managed separately.

Note

- Catalyst Center supports N+1 HA configurations for primary and secondary wireless controllers. Catalyst Center doesn't support tertiary wireless controller configurations.
- If you edit the primary wireless controller configuration, reprovision the secondary wireless controller manually with the updated configurations.

Procedure

Step 1 Ensure that you have the wireless controller in your inventory. For more information, see About Inventory, on page 78 and Add a network device, on page 130.

If the wireless controller isn't available in the inventory, use the Discovery feature to discover it. For more information, see Discover Your Network, on page 55.

Step 2 Ensure that both the wireless controllers are in the **Managed** state in the inventory. For more information, see Display information about your inventory, on page 80.

Step 3 Create enterprise and guest wireless SSIDs. For more information, see Create SSIDs for an enterprise wireless network, on page 351 and Create SSIDs for a guest wireless network, on page 366.

Step 4 If you created a wireless network profile during SSID creation, assign it to the primary wireless controller-managed site. From the main menu, choose **Design** > **Network Profiles**, and then click the corresponding **Assign Site** option for the wireless network profile.

Step 5 Provision the primary wireless controller. Choose the role as **Active Main WLC**. For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 6 Provision the secondary wireless controller. Choose the role as **Active Main WLC** and choose the secondary managed AP location same as the managed AP location for the primary wireless controller. For more information, see Provision a Cisco AireOS Controller, on page 620 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 7 Provision the APs. For more information, see Provision Cisco APs on day 1, on page 627.

Wireless mobility use cases

These topics help you understand the mobility configuration use cases for wireless networks.

Configure wireless mobility

Mobility configuration in Catalyst Center allows you to establish a tunnel between Cisco Wireless Controllers in a network allowing them to communicate with each other and dynamically share information. The mobility tunnel enables seamless roaming of clients within a wireless network. This procedure describes the steps to configure a mobility tunnel between wireless controllers for these use cases:

- Two newly added wireless controllers with the same mobility group: The two wireless controllers are newly added to Catalyst Center and are not yet provisioned.

- Two existing wireless controllers with the same mobility group: The wireless controllers are already added and provisioned on Catalyst Center and have the same mobility group name.
- Two existing wireless controllers with different mobility group: The wireless controllers are already added and provisioned on Catalyst Center and have different mobility group name.
- Two existing wireless controllers with a third wireless controller: Adding a new wireless controller to an existing mobility group between two wireless controllers.

Before you begin

- Ensure that you have the Cisco Wireless Controllers in your inventory and they are in **Managed** state. For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.
- For more information on wireless mobility configuration, see Mobility configuration overview, on page 648.

Procedure

Step 1 For newly added wireless controllers with the same mobility group, do these steps:

a) Run the **show wireless mobility summary** command to verify that there's no existing mobility tunnel between the controllers.
b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure mobility group, on page 650.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 2 For two existing wireless controllers with same mobility group, do these steps:

a) Verify that the wireless controllers have the same mobility group name configured. For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.
b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure mobility group, on page 650.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 3 For two existing wireless controllers with different mobility group, do these steps:

a) Verify that the wireless controllers have the mobility group name configured. For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.
b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure mobility group, on page 650.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

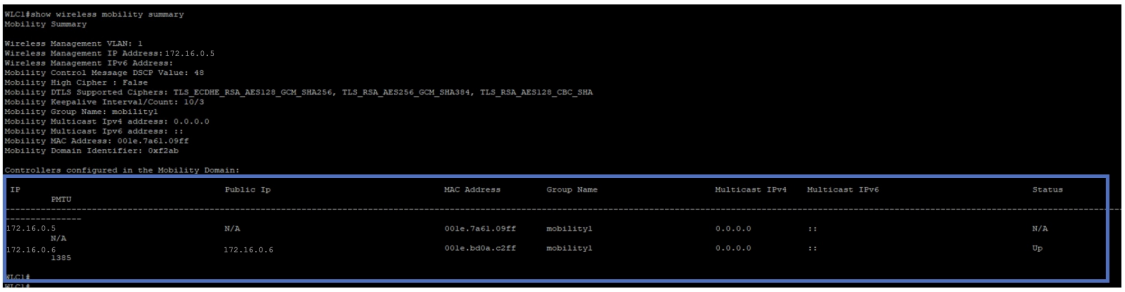
Step 4 For adding a new wireless controller to an existing mobility group between two wireless controllers, do these steps:

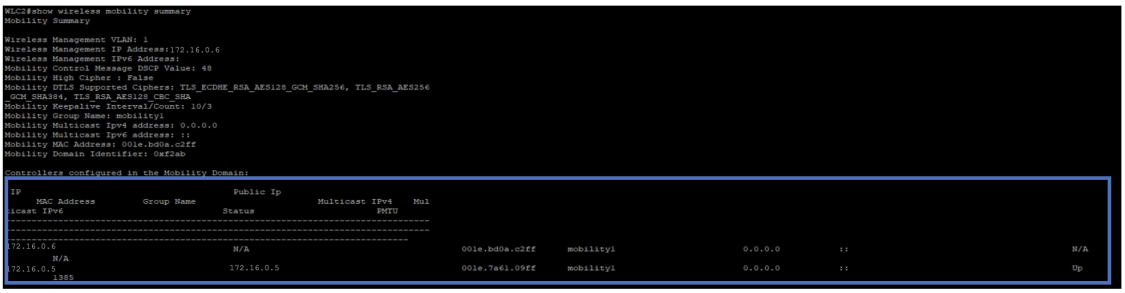
a) Verify that the existing wireless controllers have the mobility tunnel established between them by checking the mobility group name and the mobility peer information in the **Mobility** tab. For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.
b) Choose the newly added wireless controller and configure the mobility group, adding the other two existing wireless controllers as peers. For more information, see Configure mobility group, on page 650.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the existing two wireless controllers. Adding them as a peer for the newly added wireless controller automatically provisions it with the same mobility group name and peer configurations.

What to do next

After provisioning, run the **show wireless mobility summary** command on each of the controllers to verify the mobility tunnel status. This is a sample output of the command:





Configure anchor and foreign wireless mobility

The anchor and foreign wireless configuration on Catalyst Center allows you to establish wireless mobility between Cisco Wireless Controllers on different wireless networks. In an anchor and foreign setup, the foreign wireless controller encapsulates the client L3 traffic in the mobility tunnel and forwards it to the anchor wireless controller. The anchor wireless controller decapsulates the tunnel and switches the client traffic. This procedure describes the steps to configure anchor/foreign wireless mobility for these use cases:

- Configuring two newly added wireless controllers - one anchor and one foreign wireless controller.
- Configuring three newly added wireless controllers - one anchor and two foreign wireless controllers.
- Configuring three newly added wireless controllers - one foreign and two anchor wireless controllers.
- Deleting the anchor/foreign setup.

Before you begin

- Ensure that you have the Cisco Wireless Controllers in your inventory and they are in **Managed** state. For more information, see About Inventory, on page 78 and Display information about your inventory, on page 80.
- Use the **show wireless mobility summary** command to verify that there's no existing mobility tunnel between the wireless controllers.

Procedure

Step 1 Create an SSID for the wireless network and associate it with a new wireless network profile. For more information, see Create SSIDs for an enterprise wireless network, on page 351 or Create SSIDs for a guest wireless network, on page 366.

In the **Associate SSID to Profile** step, choose the **Add Profile** option and complete this configuration:

- **Profile Name**: Enter a name for the profile.
- **Fabric**: Choose **No**.
- **Do you need Anchor for this SSID?**: Choose **Yes**.

Step 2 For a scenario with one anchor and one foreign wireless controller, do these steps:

a) Assign the newly created wireless profile to the site managed by the foreign wireless controller.

To assign a site:

- From the main menu, choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, edit, and delete a site, on page 240.

b) Provision the anchor wireless controller.

- Choose the wireless controller role as **Anchor WLC** and select the anchor **Managed AP location(s)**.
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 or Provision a Cisco AireOS Controller, on page 620.

c) Provision the foreign wireless controller.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)**.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 or Provision a Cisco AireOS Controller, on page 620.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision Cisco APs on day 1, on page 627.

Step 3 For a scenario with one anchor and two foreign wireless controllers, do these steps:

a) Assign the newly created wireless profile to the sites managed by the foreign wireless controllers.

- From the main menu, choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, edit, and delete a site, on page 240.

b) Provision the anchor wireless controller.

- Choose the wireless controller role as **Anchor WLC** and select the **Managed AP location(s)** (select both foreign sites).
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 or Provision a Cisco AireOS Controller, on page 620.

c) Provision the foreign wireless controllers.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)**.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 or Provision a Cisco AireOS Controller, on page 620.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision Cisco APs on day 1, on page 627.

Step 4 For a scenario with one foreign and two anchor wireless controllers, do these steps:

a) Assign the newly created wireless profile to the sites managed by both wireless controllers (foreign and anchor).

- From the main menu, choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, edit, and delete a site, on page 240.

b) Provision the foreign wireless controller.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)** (select both foreign and anchor sites).
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 or Provision a Cisco AireOS Controller, on page 620.

c) Provision the anchor wireless controllers.

- Choose the wireless controller role as **Anchor WLC** and select the **Managed AP location(s)**.
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 or Provision a Cisco AireOS Controller, on page 620.

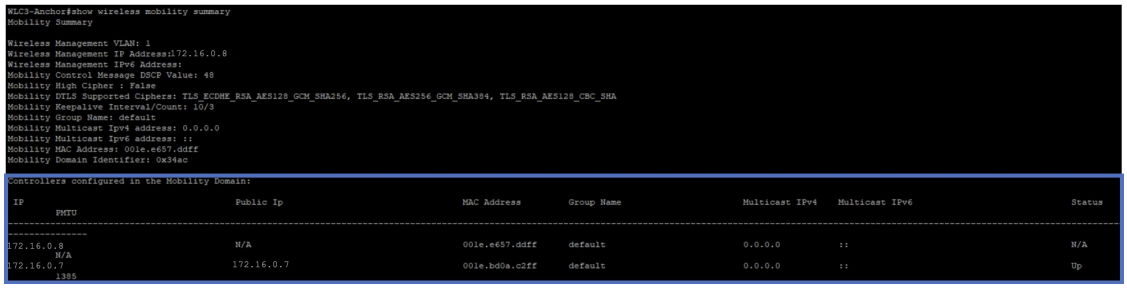
d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision Cisco APs on day 1, on page 627.

What to do next

After provisioning, Catalyst Center automatically creates a mobility tunnel between the anchor and foreign wireless controllers. Use the **show wireless mobility summary** command on each of the controllers to verify the mobility tunnel status. This is a sample output of the command:





Verify these mobility configurations on the wireless controllers:

- Both wireless controllers have the same WLAN and policy profile.
- The policy tag is created on foreign wireless controller and mapped to the AP.
- The VLAN interface is created for the anchor wireless controller and is mapped to the policy profile.

Delete the anchor/foreign setup

To delete the anchor and foreign setup, do these steps:

1. Ensure that the mobility tunnel between the anchor and foreign wireless controllers is in *up* state.
2. Delete the SSID that was created for the wireless network.
   a. From the main menu, choose **Design** > **Network Settings**
   b. Click the **Wireless** tab.
   c. From the left hierarchy tree, choose **Global**.
   d. In the **SSID** table, choose the SSID and click **Delete**.
3. Provision the foreign wireless controllers.

   In the provision **Summary** window, ensure that the SSID details are removed.

   After provisioning, Catalyst Center automatically deletes the mobility tunnel between the anchor and foreign wireless controllers and the WLAN and policy profile is deleted on all the wireless controllers.

AP management use cases

These topics help you understand the AP management use cases for wireless networks.

AP configuration

You can do these tasks for APs in Catalyst Center:

- Configure AP-level parameters and radio-level parameters for APs.
- Schedule recurring events for APs.
- Configure APs using existing templates.

For more information, see AP configurations in Catalyst Center, on page 1382.

AP refresh

You can replace old AP models with new AP models using Catalyst Center. You can replace both provisioned and unprovisioned old APs with new ones in Catalyst Center. For more information, see AP Refresh workflow, on page 1375.

Skip AP provision during Cisco Catalyst 9800 Series Wireless Controller provisioning

When you provision a wireless controller for the first time, Catalyst Center also provisions the associated APs. When you reprovision the wireless controller, Catalyst Center detects if there are any changes to these AP intent configurations:

- VLAN configurations: local VLAN, native VLAN, and AAA VLAN.
- Tag configurations: policy tag, site tag, AP profile name, flex profile name, and site tag load count.
- Failed AP wireless configuration parameters from the previous provisioning attempts.

If there are no changes to these AP intent configurations, Catalyst Center skips the provisioning of associated APs. If there are changes to the AP intent configurations, you can use the **Skip AP Provision** option to skip the AP provisioning during wireless controller reprovisioning. If you check the **Skip AP Provision** check box, Catalyst Center doesn't reprovision the existing APs and the APs managed by the wireless controller. However, the newly added APs are provisioned.

The selective AP group Resource Facing Service (RFS) translate feature optimizes wireless controller reprovisioning for AP-related configurations (such as AP tag mapping, RF tags, and flex or RF profiles) by translating only the AP intent that has changed. Out-of-band AP configurations are not automatically corrected during reprovisioning unless a compliance report explicitly flags them. To correct the AP-related out-of-band configurations to match your network intent, perform a wireless controller resynchronization and compliance run. For example, if you manually update the static tag mapping:

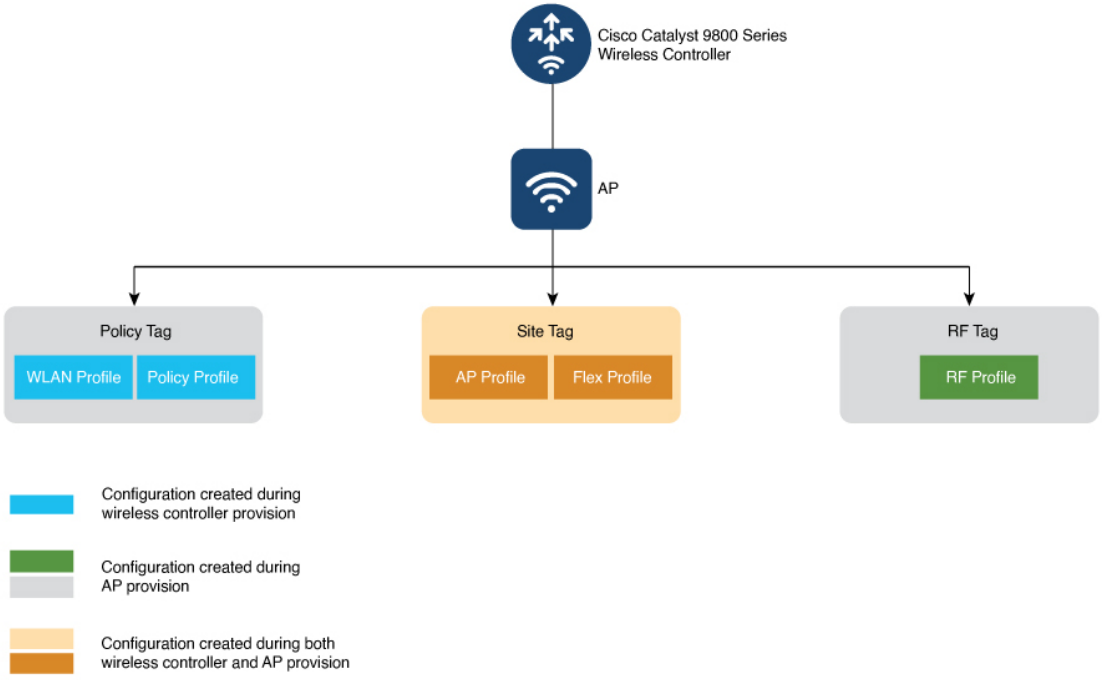
- With resynchronization and compliance run, the manual change is corrected to match the intent configuration.
- Without resynchronization and compliance run, the manual change is not corrected and only the new intent changes are applied.

To disable the selective AP group RFS translate feature, contact Cisco Technical Assistance Center (TAC).

Catalyst Center uses policy tags, site tags, and RF tags to push the wireless network configurations to individual APs through Cisco Catalyst 9800 Series Wireless Controllers.

For the first-time provisioning, Catalyst Center configures both the custom and Catalyst Center-generated site tags, policy tags, and RF tags only during the AP provisioning. For more information about the tag and flex profile configurations, see Overview of AP groups, flex groups, site tags, and policy tags, on page 465.

This figure shows how Catalyst Center processes the tags.



For information about the tags on the wireless controller, see Understand Catalyst 9800 Wireless Controllers Configuration Model.

This table lists the tags and the associated tag information during the first-time provisioning of wireless controller and APs:

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Policy tag	**Design** > **Network Settings** > **Wireless** > **SSIDs**	Autogenerated names for WLAN profile and policy profile are created.	Policy tags with the required WLAN profiles are created.

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Site tag	AP profile: **Design** > **Network Settings** > **Wireless** > **AP Profiles** Custom site tag and flex profile: **Design** > **Network Profiles** > **Add Profile** > **Wireless** > **Advanced Settings** > **Provision Group**	For nonflex configurations, an AP profile mapped to the custom site tag is created. **Note** The site tag is created and associated with the AP profile during AP provisioning.	For nonflex: • Site tags are created. • Nondefault AP profile is generated for ROW APs. • Nondefault AP profile is generated for mesh and OEAP sites.
		For flex configurations, intent configurations defined in the feature template with **IP Overlap** enabled and native VLAN configurations are created.	For flex, a nondefault flex profile is created.
RF tag	**Design** > **Network Settings** > **Wireless** > **RF Profiles**	No change	RF tag and RF profiles are created.

This table lists the tags and the associated tag information during the wireless controller and AP reprovisioning when there are changes to the AP intent configurations:

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Policy tag	**Design** > **Network Settings** > **Wireless** > **SSIDs**	• WLAN profile and policy profile mappings are configured. • Updates to policy tags are configured for the provisioned APs. • Updates to the policy tag name are configured for the provisioned APs.	• Policy tags with the required profiles are configured. • Updates to the policy tag name are configured.

Tag	Design window	Wireless Controller provision (with the Skip AP Provision unchecked)	AP provision
Site tag	AP profile: **Design** > **Network Settings** > **Wireless** > **AP Profiles** Custom site tag and flex profile: **Design** > **Network Profiles** > **Add Profile** > **Wireless** > **Advanced Settings** > **Provision Group**	Updates to site tags are configured for the provisioned APs.	Site tag, flex profile, and AP profile are created or configured.
RF tag	**Design** > **Network Settings** > **Wireless** > **RF Profiles**	Updates to the RF profile are configured.	RF tags are configured.

Note If there are no provisioned APs on a floor, tags aren't configured on the floor during the wireless controller reprovisioning.

Automated tagging for flapping APs

Catalyst Center supports automated tagging for flapping APs. When an AP flaps more than 10 times in 6 minutes, Catalyst Center assigns the AUTO_INV_EVENT_SYNC_DISABLED tag to the AP automatically. When the AP is assigned with this tag, any event on that AP is discarded. This tag prevents the unnecessary wireless controller synchronization to update the AP information for flapping APs.

If this AP doesn't flap for 10 minutes, Catalyst Center removes the AUTO_INV_EVENT_SYNC_DISABLED tag automatically.

You can view the logs for the tagging and untagging of APs on the **Audit Logs** window.

After the underlying cause of the AP flapping is resolved, we recommend that you perform a manual synchronization to immediately reflect the most current AP details. Alternatively, wait for the next scheduled synchronization to update the AP information.

Configure ROW APs

Use this procedure to configure the Rest of World (ROW) domain APs.

Procedure

Step 1 Create an AP profile with the necessary country code and configure custom site tags. For more information, see Configure additional settings for an AP profile for Cisco IOS XE devices, on page 431 and Add AP groups, flex groups, site tags, and policy tags to a network profile, on page 475.

Note If you don't create an AP profile, Catalyst Center automatically generates the AP profile with the country code of the selected site and site tags for the ROW AP during AP provisioning or AP PnP onboarding.

Step 2 Add support for the country of operation to the country list on the wireless controller. You must configure at least one site from the country of operation as the managed AP location for the wireless controller. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 3 If the wireless controller is not already provisioned with the configurations in Step 1, on page 1445 and Step 2, on page 1446, provision the wireless controller. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656.

Step 4 Configure the AP parameters. For more information, see Configure APs, on page 1382.

Step 5 Provision the AP. For more information, see Provision Cisco APs on day 1, on page 627.

Note Onboarding a ROW AP to a site with existing APs may disrupt the services of the existing APs for a brief period.

What to do next

To verify the AP configuration, use the **show ap summary** command. This is a sample output of the command.

```
C9800LC-94#show ap summary
Number of APs: 4

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model           Ethernet MAC   Radio MAC      CC   RD   IP Address                                 State       Location
-------------------------------------------------------------------------------------------------------------------------------------------------------------
AP68-C9130I-0D40                 3     C9130AXI-B         3c41.[redacted] 1416.[redacted] IN   -B   [redacted]                                 Registered  Texas
C9130AXI-5A40                    3     C9130AXI-D         548a.[redacted] 488b.[redacted] IN   -D   [redacted]                                 Registered  DEFAULT
C9136I-E1F4                      4     C9136I-ROW         4891.[redacted] 6cd6.[redacted] IN   -RW  [redacted]                                 Registered  DEFAULT
C9115AXI-4AD4                    2     C9115AXI-D         6c41.[redacted] a4b4.[redacted] IN   -D   [redacted]                                 Registered  DEFAULT
```

This command displays the country code (CC) and regulatory domain (RD) for the APs. For ROW APs, the regulatory domain is **-RW**.

Note For a ROW AP, if the country code in the command output is **--**, it indicates that the country code is not available for the AP. The operational status of all the radios for the ROW APs without a country code is **down**. You must provision the ROW AP to configure the country code for the ROW AP.

Configure wireless mesh network

In a Cisco wireless mesh network architecture, APs operate in one of these ways:

- Root APs (RAP): Connected to the wired network.
- Mesh APs (MAP): Communicates with other MAPs and RAPs using wireless connections.

The workflow for configuring a wireless mesh network involves these main steps:

1. Wireless controller provisioning: Configure a mesh profile, configure the AP authorization list and provision the wireless controller.
2. AP configuration: Configure AP in bridge mode and deploy.
3. AP provisioning: Configure the mesh role for AP (RAP or MAP) and provision the AP.

Before you begin

All APs are configured and shipped as MAPs. To use the AP as a RAP, you must reconfigure it as a RAP during AP provisioning. A mesh network must contain at least one RAP. For more information on Cisco Wireless Controller configuration and AP configuration for wireless mesh networks, see About wireless mesh networks, on page 449.

Procedure

Step 1 In the Catalyst Center device inventory (**Provision** > **Inventory**), ensure that the wireless controllers and APs are in managed state and assigned to the respective sites.

Step 2 Create an AP profile with mesh settings. For more information, see Configure mesh settings for an AP profile for Cisco IOS XE devices, on page 429 and Configure mesh settings for an AP profile for Cisco AireOS devices, on page 434.

Step 3 Add the AP Ethernet MAC address to the AP authorization list. For more information, see Create an AP authorization list, on page 417.

Step 4 Provision the Cisco Wireless Controller. For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 656 and Provision a Cisco AireOS Controller, on page 620.

In the provision configuration window, select the **AP Authorization List** defined in Step 3 and choose the option for authorizing only the mesh access points.

Step 5 (Optional) In the **Configure Access Points** workflow, select the APs and change the AP mode to **Bridge/Flex+Bridge** mode if they are in **Local/Flexconnect** mode. For more information, see Configure APs, on page 1382.

Step 6 Provision the APs. For more information, see Provision Cisco APs on day 1, on page 627.

- For RAPs, choose the **Mesh Role** as **RAP (Root AP)**.
- For MAPs, choose the **Mesh Role** as **MAP (Mesh AP)**.

What to do next

You can verify the mesh configurations on the Cisco Wireless Controller using these commands:

- AP Ethernet MAC address: **show run | inc username**.
- AP mesh role (MAP/RAP) after provisioning: **show wireless mesh ap summary**.
- Site tag details: **show wireless tag site detailed <site tag name>**.
- AP profile: **show run | section ap profile**.
- Wireless mesh configurations:
  - **show wireless profile mesh summary**

- **show wireless profile mesh detailed <mesh profile name>**

AP migration from a wireless controller to another wireless controller

You can migrate APs from one wireless controller to another wireless controller with the same floors in the network hierarchy. For more information, see Migrate APs from a Wireless Controller to another Wireless Controller, on page 629.

AP replacement using RMA workflow

You can replace a faulty access point in the network using the Catalyst Center Return Material Authorization (RMA) feature. The RMA workflow lets you replace failed devices quickly, thus improving productivity and reducing operational expense. For wireless APs, the replacement device is assigned to the same site, provisioned with primary wireless controller, RF profile, and AP group settings, and placed on the same floor map location in Catalyst Center as the failed AP.

For more information, see Replace a faulty access point, on page 211.

Onboard APs using PnP for non-intent-based deployments

Use this procedure to onboard and provision APs using Plug and Play (PnP) for deployments that:

- do not use intent-based configurations and
- are not provisioned with a network profile from Catalyst Center

The non-intent-based configurations include the Assurance use case and Per-Device Configurations.

Before you begin

- Ensure that the Cisco Catalyst 9800 Series Wireless Controller is added to the inventory.
- Configure the DHCP server with Option 43 for PnP. This option informs the network device of the IP address of the Catalyst Center controller.
- Ensure that the APs are in the factory reset state.
- Ensure the network connectivity between APs, Catalyst Center, and wireless controller.

Procedure

Step 1 Create a regular day-zero template for onboarding APs using PnP.

a) Use these configurations:

- Template Name: Enter a name for the template
- Project Name: **Onboarding Configuration**
- Deployment Type: **Day 0**
- Template Language: **Jinja**

- Software Type: **IOS-XE**
- Device Family: **Wireless Controller**
- Device Model: **Cisco Catalyst 9800 Wireless Controllers**

For more information, refer to Create a regular template, on page 487.

b) Add these configurations in the template, save, and commit the changes:

- Primary wireless controller IP address
- Primary wireless controller name
- Secondary wireless controller IP address
- Secondary wireless controller name
- Policy tag name
- Site tag name
- RF tag name

For more information, refer to Edit templates, on page 491.

Catalyst Center pushes these configurations to APs during PnP claim.

For example, add these configurations in the template:

```
{
  "primaryWlcIP": "10.0.0.1",
  "primaryWlcName": "Primary-WLC",
  "secondaryWlcIP": "10.0.0.5",
  "secondaryWlcName": "Secondary-WLC",
  "policyTagName": "default-policy-tag",
  "siteTagName": "default-site-tag",
  "RFTagName": "default-rf-tag"
}
```

Step 2 Claim the APs using PnP.

a) Do not assign the APs to a site.

b) Select the day-zero template that you created for AP onboarding.

For more information, refer to Provision a wireless controller, on page 606.

After PnP claim, the configuration is pushed to AP and it joins the corresponding wireless controller. The AP appears in the inventory.

What to do next

In the AP console, use the **show pnp log** to verify the PnP claim. A sample output of the command is:

```
#show pnp log
722 - pnp.agent - DEBUG - Setting sid from stored value 551de96a-c719-44f0-8964-16b150f7325d
APC414.A2FB.0CB0#
PNP CONFIG - HOST NAME   : APC414.A2FB.0CB0
PNP CONFIG - PRI WLC IP  : 10.0.0.1
PNP CONFIG - SEC WLC IP  : 10.0.0.5
```

```
PNP CONFIG - PRI WLC NAME: Primary-WLC
PNP CONFIG - SEC WLC NAME: Secondary-WLC
PNP CONFIG - Policy Tag  : default-policy-tag
PNP CONFIG - Site Tag    : default-site-tag
PNP CONFIG - RF Tag      : default-rf-tag
PnP: Config Upgrade received. Start CAPWAP discovery
```

Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers

Catalyst Center can learn configurations from an existing Cisco Catalyst 9800 Series Wireless Controller and save the configurations as configuration profiles. Configuration profiles can be learned from wireless controllers that are provisioned using either Per-Device Configurations, provisioned using intent-based network configurations, or available in the inventory without being provisioned. You can provision multiple wireless controllers using configuration profiles, ensuring consistent settings and standardized deployment.

Note This feature is in beta and requires feature enablement. To enable the feature, contact Cisco TAC. If this feature is not enabled, the options for wireless controller-related configurations are unavailable or dimmed.

Configuration profiles are version-specific. The profiles learned from a wireless controller running a specific Cisco IOS XE Release can be applied only to wireless controllers running the same version. Configuration profiles are not associated with site or network and can be used across different networks.

For more information about campus networks, refer to Provision Campus Networks, on page 1089.

Prerequisites

- Wireless controllers must be running Cisco IOS XE Release 17.12 or later.
- Per-Device Configurations must be enabled on the wireless controllers included in the campus network. For more information, refer to Enable Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller, on page 674.
- Wireless controllers and APs must be added to inventory and assigned to the required sites.

Standardize complete configuration for wireless controllers on day zero

Ensure uniform initial configuration for all wireless controllers in your network by copying device configurations from an existing wireless controller and standardizing the setup.

Before you begin

Refer to Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers, on page 1450.

Use this procedure to copy the configurations from a wireless controller and apply them to all other wireless controllers in your network to ensure uniform day-zero configurations.

Procedure

Step 1 Create a network and add the wireless controllers that need to be included in the network.

For information about creating a network with wireless controllers, refer to Create a network, on page 1091.

Step 2 Learn configuration profiles from an existing wireless controller.

For more information, refer to Learn configuration profiles from a wireless controller, on page 1097.

Step 3 Standardize the configuration for wireless controllers in the network.

a) Assign the configuration profiles to the required wireless controllers, resolve any validation errors that impact provisioning, and schedule the provisioning.

For more information, refer to Assign configuration profiles to a wireless controller, on page 1107.



Note Ensure that the wireless controller is running the same Cisco IOS XE Release as the wireless controller from which configuration profile is learned.

b) (Optional) Edit the configuration profile assignment for wireless controllers.

For more information, refer to Edit configuration profile assignment for a wireless controller, on page 1108.

Step 4 Verify that the configuration is pushed to the wireless controllers.

a) From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
b) Click the network name to view network details.
c) Click the **Devices** tab.
d) Click **wireless controllers**.
e) Click the device name.
f) In the **Sync Status** column, verify that the status is **In Sync** for the wireless controller.

Step 5 Configure the tags (site tag, policy tag, and RF tag) for APs associated with the wireless controllers using Per-Device Configurations.

For more information, refer to Manage APs associated with a Cisco Catalyst 9800 Series Wireless Controller, on page 676.

Standardize partial configuration for wireless controllers on day zero

Apply and customize partial configuration profiles for wireless controllers, ensuring only required configurations are provisioned during initial deployment.

Use this procedure to customize configuration profiles learned from existing wireless controllers. For example, if a learned profile includes ten SSIDs but only two are needed for a site, modify the profile to match site requirements.

Before you begin

Refer to Campus networks configuration use cases for Cisco Catalyst 9800 Series Wireless Controllers, on page 1450.

Procedure

Step 1 Create a network and add the wireless controllers that need to be included in the network.

For information about creating a network with wireless controllers, refer to Create a network, on page 1091.

Step 2 Learn configuration profiles from an existing wireless controller.

For more information, refer to Learn configuration profiles from a wireless controller, on page 1097.

Step 3 Standardize the partial configuration for the required wireless controllers in the network.

a) Duplicate the configuration profile for wireless profiles.

For more information, refer to Manage configuration profiles, on page 1092.

b) (Optional) Edit or delete the configurations in the duplicated profile as needed.

For information about editing or deleting a configuration profile for the wireless controller, refer to Manage configuration profiles, on page 1092.

For example, if you want to use only two out of ten SSIDs in the configuration profile, delete the eight SSIDs that you do not need.

c) Assign the configuration profiles to the required wireless controllers, resolve any validation errors that impact provisioning, and schedule the provisioning.

For more information, refer to Assign configuration profiles to a wireless controller, on page 1107.

Step 4 Verify that the configuration is pushed to the wireless controllers.

a) From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
b) Click the network name to view network details.
c) Click the **Devices** tab.
d) Click **wireless controllers**.
e) Click the device name.
f) In the **Sync Status** column, verify that the status is **In Sync** for the wireless controller.

Manage configurations for a wireless controller on day *n*

Maintain, update, or remove configurations for wireless controllers by updating configuration profiles.

Use this procedure to add, edit, or delete a setting in a configuration profile for a wireless controller on day n. For example, use this procedure to create an SSID for Wi-Fi 7 clients.

Procedure

Step 1 Manage your configurations in the configuration profile.

a) Edit or delete configurations in the configuration profile for the wireless profile as needed.

For information about editing or deleting a configuration profile for the wireless controller, refer to Manage configuration profiles, on page 1092.

For example, click **Add** in the **WLAN Profiles** table to add an SSID for Wi-Fi 7. After you create the SSID, map it to the policy tag.

The **Sync Status** for the wireless controller (refer to Step 2, on page 1453) changes to **Out of sync** as the configuration profile that is already assigned and provisioned on the wireless controller is modified.

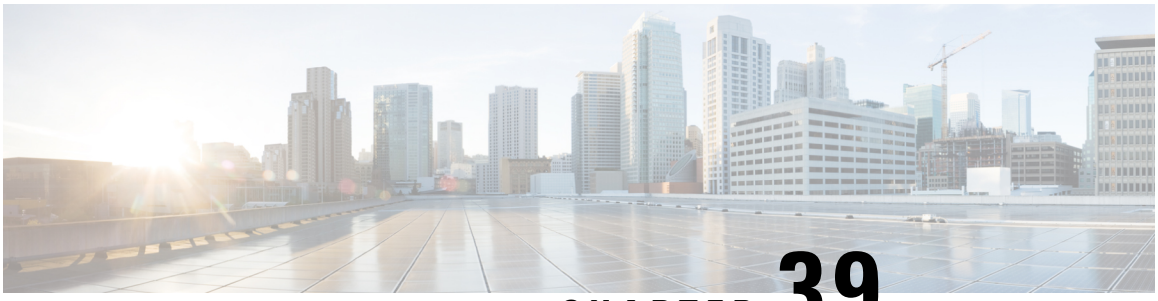
b) Verify your updated configurations, resolve any validation errors that impact provisioning, and reprovision the wireless controller with the updated configuration profile.

The **Change type** column identifies the status of each configuration during provisioning. This column displays **Modify** for existing configurations that have been updated, **Add** for newly created configurations, and **No changes** for configurations that are already synchronized and not updated.

For more information, refer to Edit configuration profile assignment for a wireless controller, on page 1108.

Step 2 Verify that the configuration is pushed to the wireless controllers.

a) From the main menu, choose **Provision** > **Campus Network** > **Networks & Configuration Profiles**.
b) Click the network name to view network details.
c) Click the **Devices** tab.
d) Click **wireless controllers**.
e) Click the device name.
f) In the **Sync Status** column, verify that the status is **In Sync** for the wireless controller.



CHAPTER 39

Manage Energy on Your Network

- Overview, on page 1455
- Manage energy on network devices, on page 1455
- Use the Energy Management dashboard, on page 1457
- Generate a report of energy management for network devices, on page 1458
- View energy consumption of network devices, on page 1459
- Carbon emissions of network devices, on page 1460
- View energy savings, on page 1461
- Compare energy across sites, on page 1462

Overview

Catalyst Center offers a range of energy management capabilities that are designed to help organizations optimize their energy usage, reduce costs, and improve sustainability. Catalyst Center energy management solutions offer these key features:

- **Cost optimization**: You can regularly review energy consumption data and adjust strategies for cost savings.
- **Sustainability**: The energy management capabilities help you support your sustainability initiatives by reducing your carbon footprint through efficient energy use.
- **Assess high-consumption devices**: Catalyst Center provides energy audit to identify high-consumption devices and patterns. This assessment helps you replace outdated network devices with energy-efficient models.
- **Reporting and analytics**: Catalyst Center provides detailed reports and analytics on energy usage. Use them to identify trends, track savings, and support sustainability initiatives.

Manage energy on network devices

Use Energy Management to monitor the cost, energy consumption, and carbon emissions of your network.

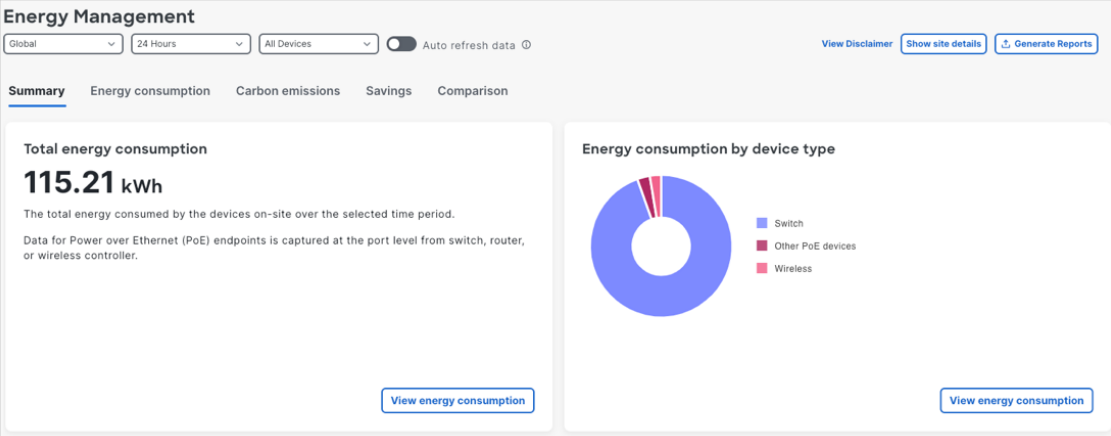
This section explains the options available in the **Energy Management** window.

Procedure

Step 1 From the main menu, choose **Energy Management**.

Catalyst Center displays energy consumption for all network devices for the last 24 hours by default.

Important Data and other information generated in this dashboard are subject to the disclaimer provided in the **Disclaimer** slide-in pane. Click the **View Disclaimer** link to view this pane.



Step 2 Choose a site from the **Global** drop-down list to view its energy consumption.

Step 3 You can view energy consumption for the last 24 hours or seven days. To change the time range, choose **7 Days** from the **24 Hours** drop-down list and click **Apply**.

You can also change the date and time in the **Start Time and End Time** area to view the energy consumption for a specific day or week.

Step 4 To view the energy consumption of the switches, routers, access points, or other Power over Ethernet (PoE) devices, choose the device type from the **All Devices** drop-down list.

Step 5 Enable the **Auto refresh data** toggle button to refresh data on the **Energy Management** window.

Data refreshes every 5 minutes. Click the pause button to temporarily stop data refresh.

Step 6 Click **Show site details** button to view detailed information for all sites.

You can view carbon intensity, energy consumption, estimated emissions, and the estimated cost for all sites.

Sites (3)

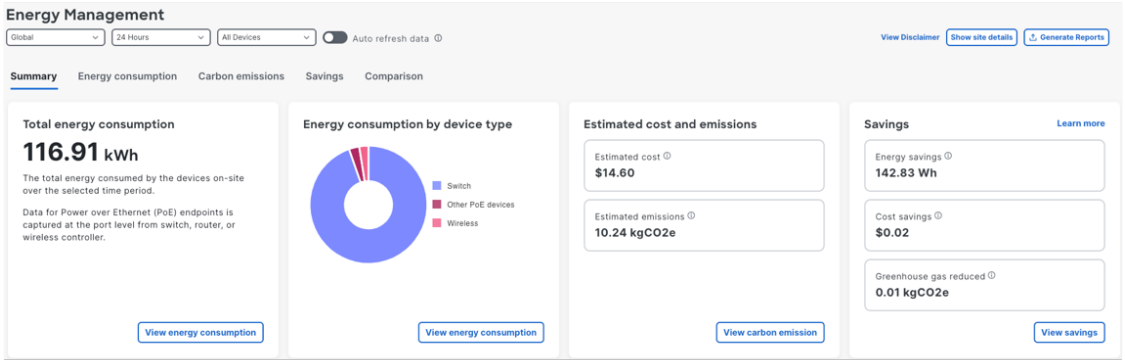
Site	Carbon Intensity (gCO2e/kWh)	Energy Consumption (kWh)	Estimated Emissions (kgCO2e)	Estimated Cost ($)
Global	150.71	37.87	5.71	5.30
San Jose	192.10	21.79	4.18	3.29
Kanata	94.67	16.09	1.52	2.01

You can compare values between different sites in this table. To view details such as energy consumption, carbon intensity, estimated emissions, and consumption costs for the buildings and floors of a site, click the site name hyperlink.

Click the map view icon ( ) to display the sites on a map. To view details such as energy consumption, carbon intensity, emissions, and estimated consumption cost, hover over a site.

Use the Energy Management dashboard

This section describes the components of the Energy Management dashboard:

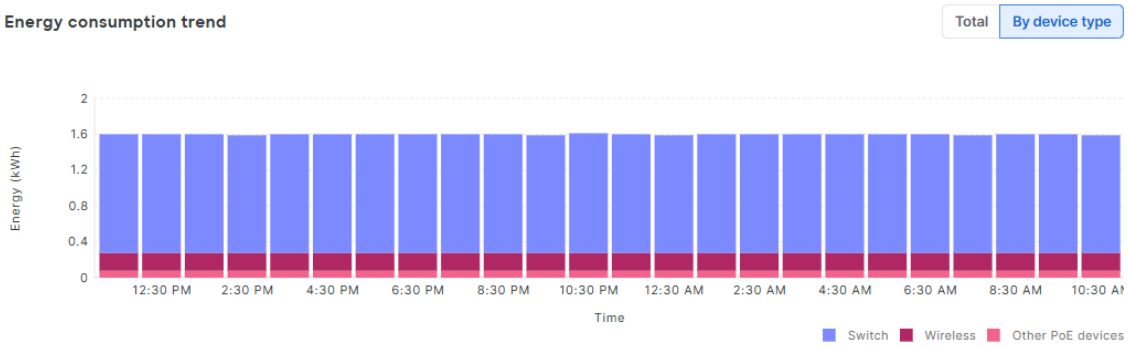


- **Total energy consumption**: This dashlet displays the amount of energy consumed by the devices for a chosen site and time range.
- **Energy consumption by device type**: This dashlet displays the energy consumed by each device type for a chosen site and time range.
- **Estimated cost and emissions**:
  - **Estimated cost**: Displays the estimated cost of the energy consumed based on the Electricity Maps (if available) or the International Energy Agency (IEA) data.
  - **Estimated emissions**: Displays carbon emissions of the energy consumed in kilograms of carbon dioxide equivalent (kgCO2e).
- **Savings**: This dashlet displays the energy savings, cost savings, and reduced greenhouse gas emissions.

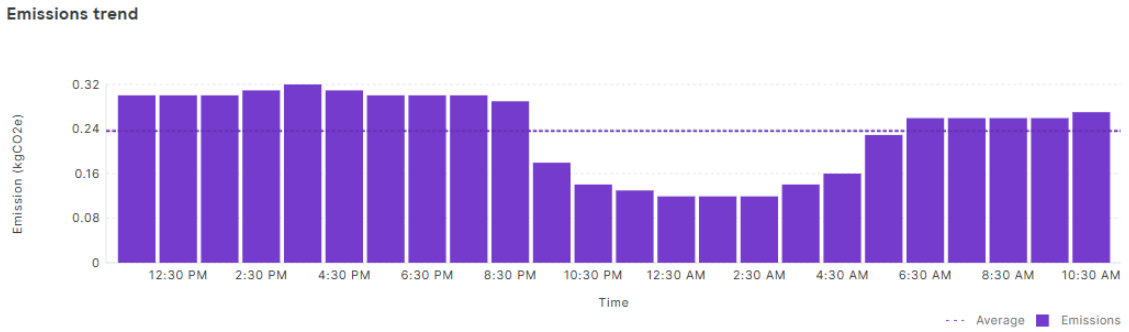
Note You can view savings achieved only through APs operating in power save mode.

For information on how to configure APs in power save mode on Catalyst Center, see Create an AP power profile, on page 436.

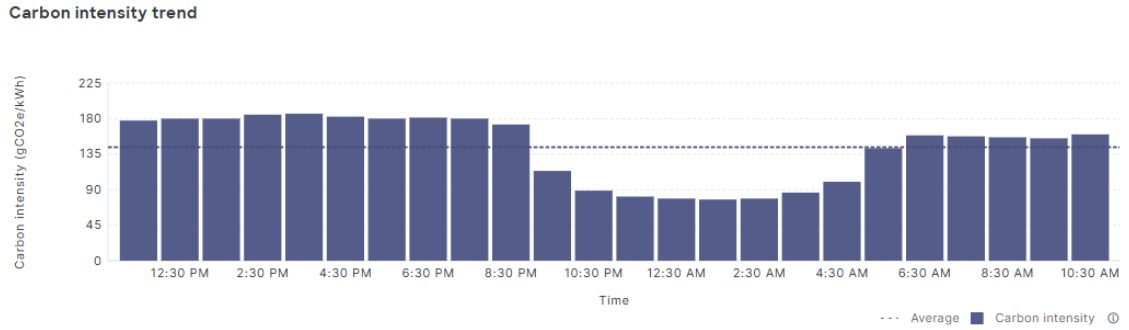
- **Energy consumption trend**: Displays the trend of energy consumed over a range of time. Click the toggle button to view energy consumption trends for all devices or by device type.



- **Emissions trend**: Displays the trend of carbon emissions for the chosen devices over a range of time.



- **Carbon intensity trend**: Displays the trend of carbon intensity over a range of time. Carbon intensity refers to the amount of carbon dioxide (CO_2) emissions produced per unit of energy output.



Click the **Energy consumption**, **Carbon emissions**, **Savings**, and **Comparison** tabs to view detailed information for each category.

Generate a report of energy management for network devices

Catalyst Center provides a consolidated energy management report. The report shows energy consumption, cost, carbon emissions, and the carbon intensity data of your network devices.

For more information, see "Run a Network Devices Report" in the *Cisco Catalyst Center Platform User Guide*.

View energy consumption of network devices

Catalyst Center allows you to assess the energy consumption of network devices. Use this assessment to manage operational costs and reduce environmental impact.

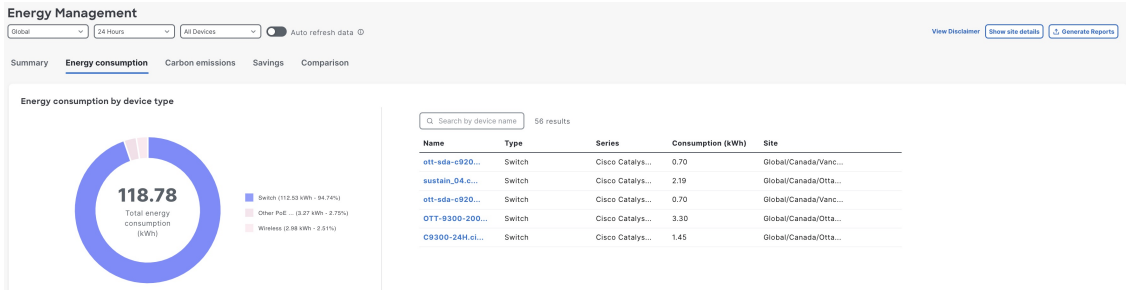
The factors that affect energy consumption in network devices include:

- **Device Type**: Switches, routers, APs, and other PoE devices, each having different energy requirements.
- **Usage Patterns**: Devices operating at full capacity or under significant load typically consume more energy.
- **Environmental Conditions**: Operating temperature and humidity can affect energy usage.

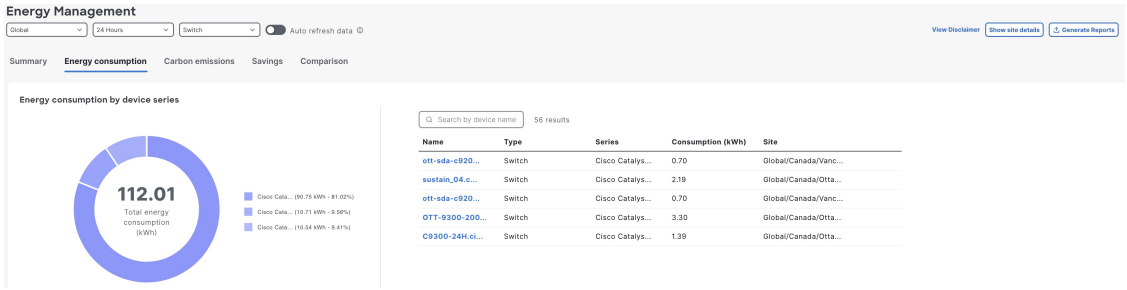
From the main menu, choose **Energy Management** > **Energy consumption**.

The Energy Consumption dashboard includes these sections:

- **Energy consumption by device type** displays the total energy consumption for all devices and individual device types.

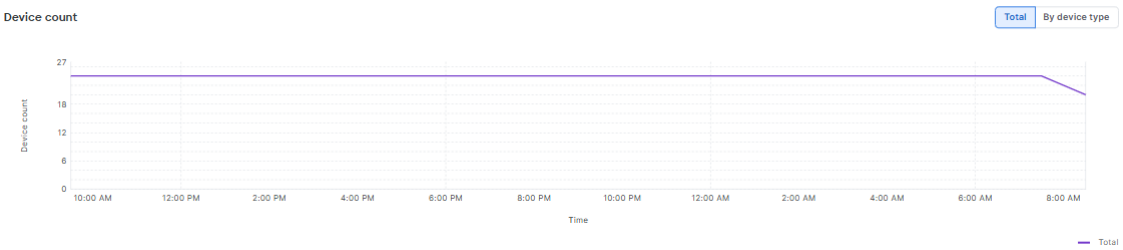


From the **All Devices** drop-down list, choose the device type to view the energy consumption for device series.



The table lists all the devices and provides information such as device type, device series, the site, and the energy consumed by the device.

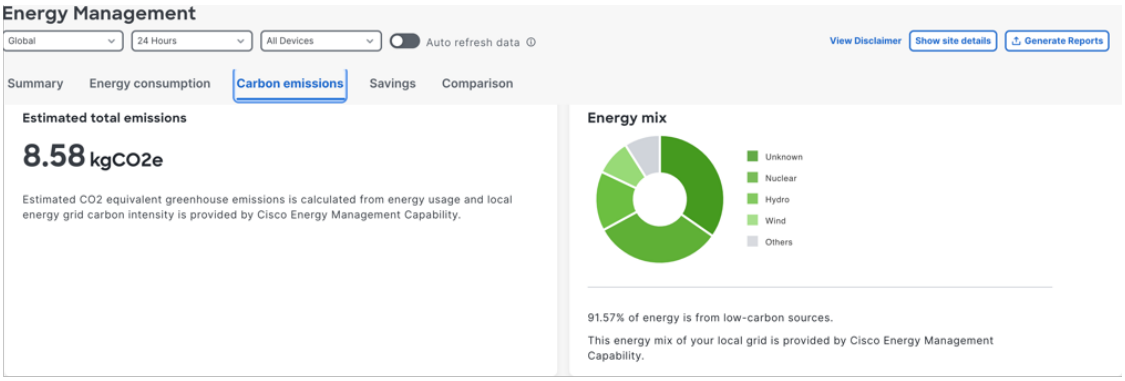
- **Energy consumption trend** displays a graphical representation of energy consumed over a time range.
- **Device count** displays the total number of devices and the number of devices based on device type over a time range. This graph displays only the number of devices that report energy data. The device count excludes devices that do not report energy data.



Carbon emissions of network devices

Carbon emissions are the release of carbon—especially carbon dioxide (CO_2)—into the atmosphere. These emissions significantly contribute to climate change by increasing the greenhouse effect. This results in global warming and various environmental impacts.

The Energy Management feature provides estimated carbon emissions data for your network devices and gives insights over a selected time range.

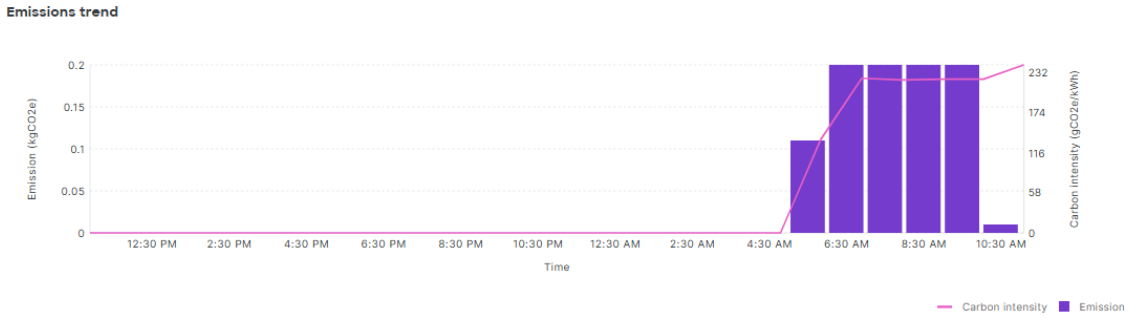


To view the carbon emissions dashboard, click the menu icon in the top-left corner. Then choose **Energy Management** > **Carbon emissions**. The dashboard displays these sections:

- **Estimated total emissions**: This dashlet displays the estimated greenhouse gas emissions, specifically carbon dioxide (CO_2) equivalents, based on energy consumption and the carbon intensity of the local energy grid.
- **Energy mix**: This dashlet displays energy generated from different sources, such as gas power plants, nuclear power plants, hydroelectric dams, wind discharge, and battery discharge.

  Electricity generation, especially when using fossil fuels such as coal or natural gas, is a major source of greenhouse gas emissions including CO_2.

  Nuclear power plants, hydroelectric dams, and wind turbines are clean electricity sources with zero to negligible carbon emissions. These sources appear in shades of green. Electricity from gas power plants is shown in shades of red to indicate its higher carbon footprint. Sources in gray show electricity from unknown sources.
- **Emissions trend**: This area displays a graphical representation of the carbon emissions and carbon intensity over a time range.



View energy savings

The Energy Management Savings dashboard shows the estimated cost and energy savings, and the estimated reduction of gas emissions when power-save mode is applied to APs.

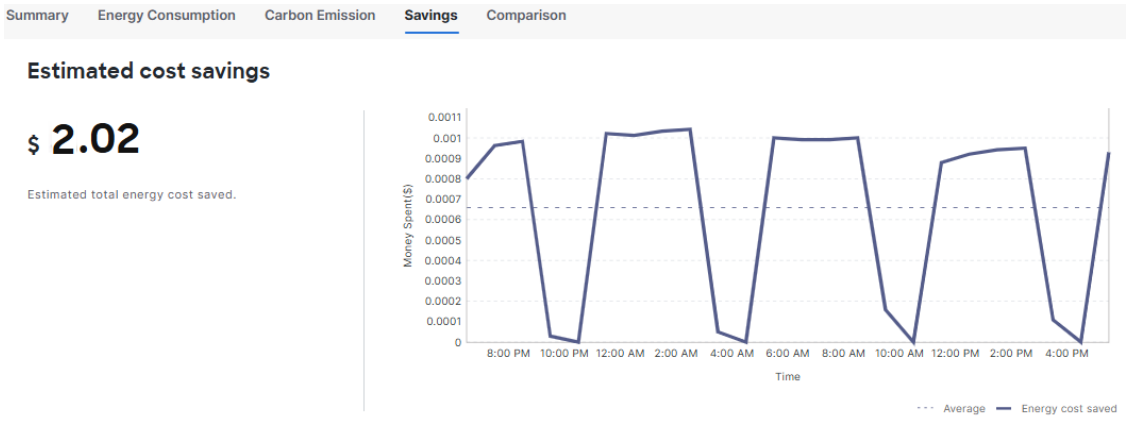
From the main menu, choose **Energy Management** > **Savings** to monitor and analyze savings.

Note The dashboard captures only the savings achieved when APs operate in power-save mode.

For information on how to configure APs in power-save mode on Catalyst Center, see Create an AP power profile, on page 436.

The Savings dashboard contains these sections:

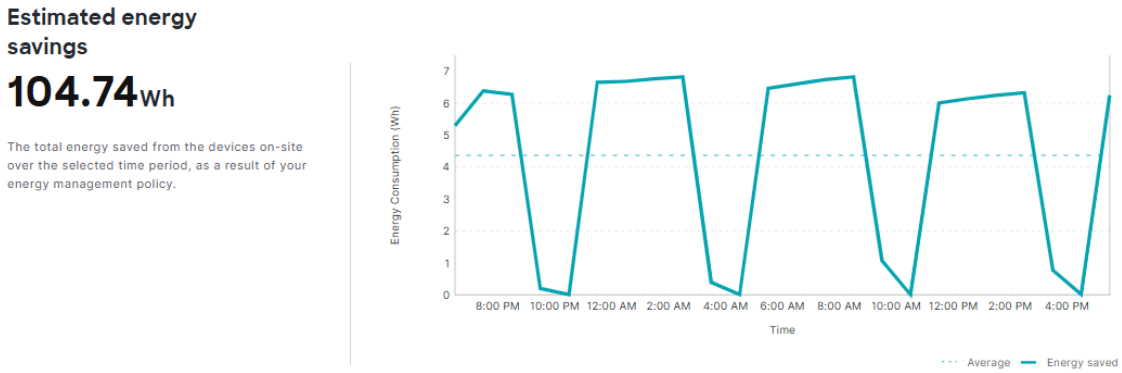
- **Estimated cost savings**: This area displays the estimated cost savings achieved due to the reduced energy consumption. It also displays a graph showing the money spent over a period of time.



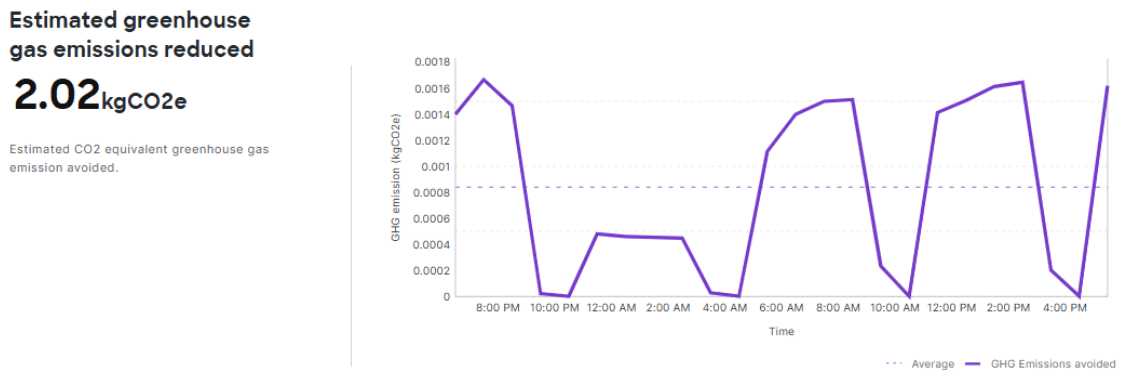
- **Estimated energy savings**: This area displays the estimated energy savings achieved in watt-hours (Wh). You can configure APs to operate in normal mode or in power-save mode. The savings value is calculated by subtracting the energy consumed in power-save mode from the energy consumed in normal mode. This savings is calculated based on live, switch-reported energy consumption.

  This metric is more granular than the **Assurance** > **PoE dashboard** > **Estimated AP Power Savings** value, which is based on power samples. In the PoE dashboard, Assurance samples the data once per

hour and calculates energy consumption from these samples. This provides a higher-level approximation than the energy savings displayed in the Energy Management window.



- **Estimated greenhouse gas emissions reduced**: Energy consumption often leads to greenhouse gas (GHG) emissions. This area displays the amount of carbon dioxide (CO_2) and other greenhouse gases reduced due to decreased energy consumption.

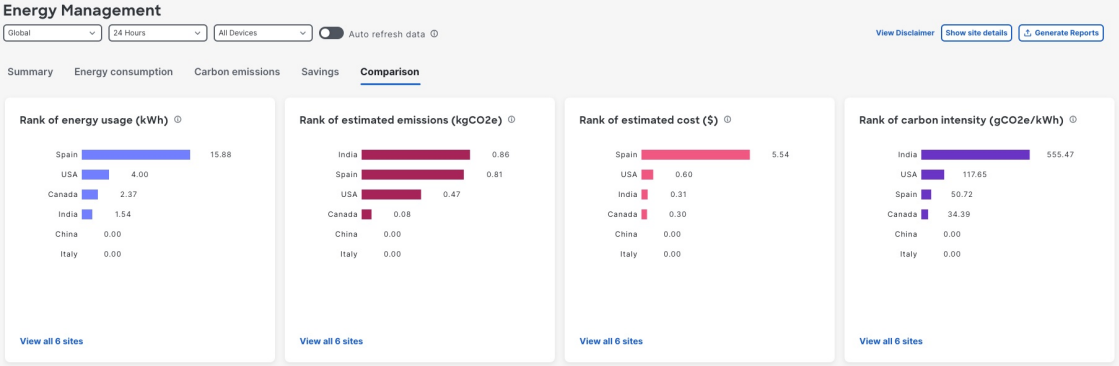


Reducing GHG emissions contributes to mitigating climate change and improving air quality.

Compare energy across sites

To analyze energy across your network, Catalyst Center ranks sites by energy consumption, estimated emissions, cost, and carbon emissions intensity.

From the main menu, choose **Energy Management** > **Comparison**.

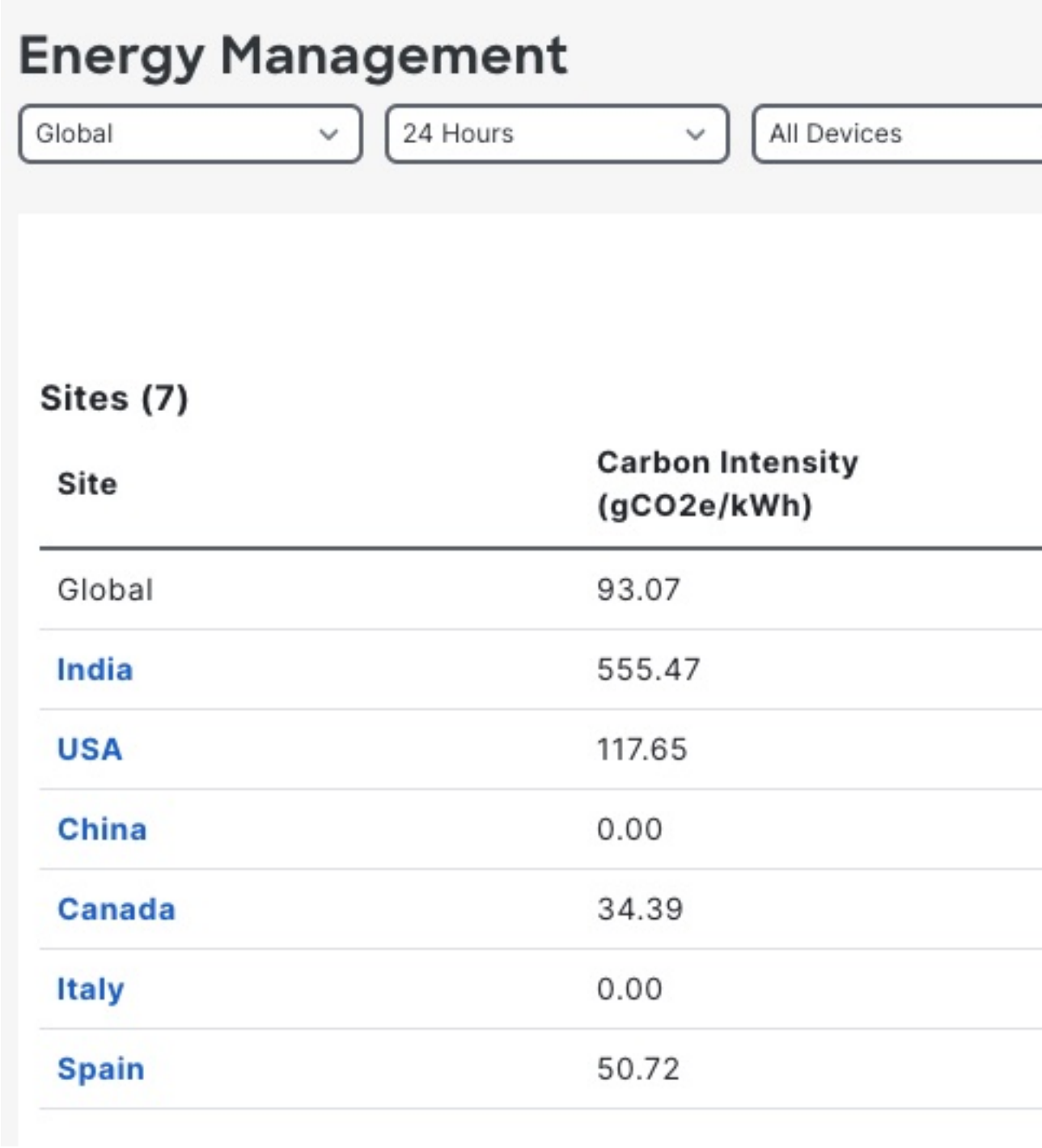


The **Comparison** dashboard ranks sites by energy consumption, estimated emissions, cost, and carbon emissions intensity. To view the site details for a specific rank, click the corresponding link.

Sites by kWh energy usage (6)

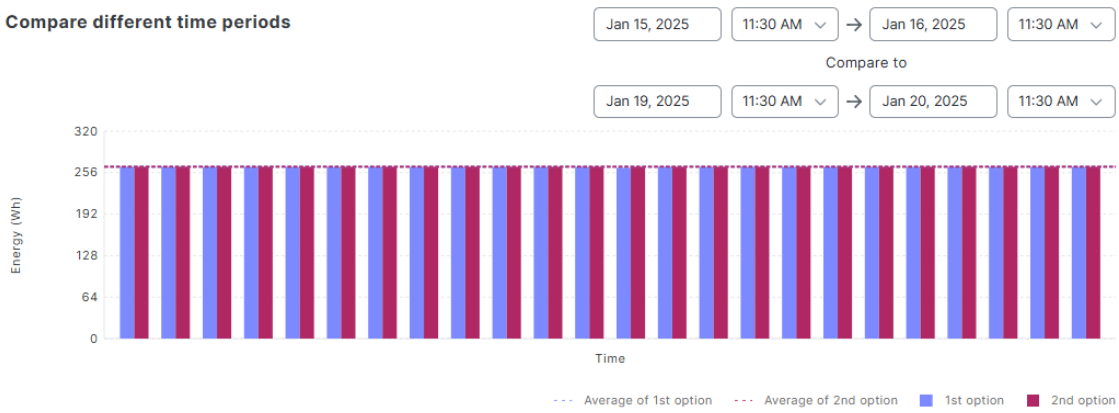
Rank	Site	Energy consumption (kWh)	Emissi (kgCO2
1	Spain	15.88	0.81
2	USA	4.00	0.47
3	Canada	2.37	0.08
4	India	1.54	0.86
5	China	0.00	0.00
5	Italy	0.00	0.00

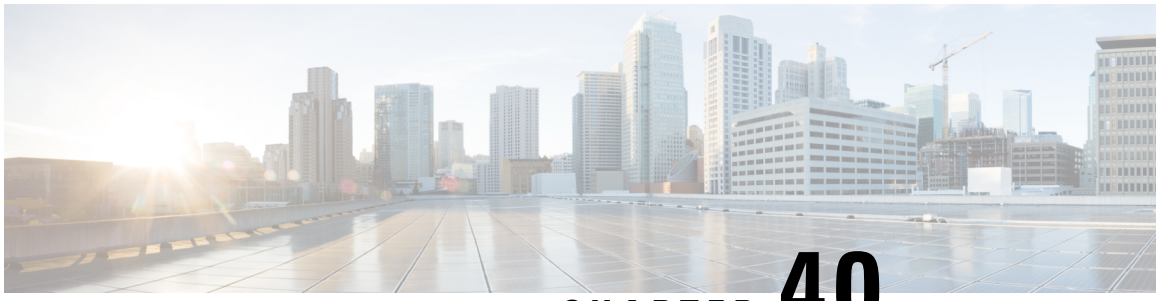
Click **Show site details** to view the name and rank of each site.



Click a site name to view more detailed information for that site.

The **Compare different time periods** area shows a graph of energy consumption in watt-hours over selected time ranges.


Compare different time periods
Jan 15, 2025
11:30 AM
Jan 16, 2025
11:30 AM
Compare to
Jan 19, 2025
11:30 AM
Jan 20, 2025
11:30 AM
320
256
192
128
64
0
Energy (Wh)
Time
Average of 1st option
Average of 2nd option
1st option
2nd option



CHAPTER 40

Troubleshoot Catalyst Center Using Data Platform

- About Data Platform, on page 1467
- View or update Collector configuration information, on page 1468
- View data retention settings, on page 1469
- View pipeline status, on page 1469

About Data Platform

Data Platform provides tools that can help you monitor and troubleshoot Catalyst Center applications. **Data Platform** displays synthesized data from various inputs to help you identify patterns, trends, and problem areas in your network. For example, if something goes wrong in your network, you can quickly get answers to questions such as whether a pipeline is in an error state and what is the real-time traffic flow in a particular area.

The Admin user has Read and Write access to Data Platform administration section. The Observer user has only Read access.

The main areas of Data Platform include:

- **Collectors**: Collects a variety of network telemetry and contextual data in real time. As data is ingested, Catalyst Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas. See View or update Collector configuration information, on page 1468.
- **Store Settings**: Indicates how long data is stored for an application. See View data retention settings, on page 1469.
- **Pipelines**: Allows Catalyst Center applications to process streaming data. A data pipeline encapsulates an entire series of computations. These computations accept input data from external sources, transform the data to provide useful intelligence, and produce output data. You can view the status of pipelines and quickly identify any problem areas. See View pipeline status, on page 1469.

- **Task Managers**: You can view the list of Task Managers with details such as Last Heart Beat, All Slots, and Free Slots. You can export the details as a CSV file.

View or update Collector configuration information

Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, Catalyst Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas.

Procedure

Step 1 From the main menu, choose **System** > **Data Platform**.

Step 2 Click **Collectors**. The dot next to each collector indicates its overall status.

Step 3 To view additional details, click a collector name.

The appropriate *Collector* page appears. By default, Catalyst Center displays the **Configurations** tab, which displays the list of current configurations.

Step 4 To view, update, or delete a configuration, click a specific configuration name.

Step 5 To add a new configuration, click **+ Add** in the **Configurations** tab.

Step 6 Enter the required information for the configuration in the slide-in pane.

Step 7 (Optional) For some collectors, such as the wireless collector, you can check the **Anonymize** check box to scramble the hostname and user ID in the **Client Health** window with a one-way hash that cannot be decrypted.



Important If you want to anonymize your data, make sure that you check the **Anonymize** check box before you discover devices with the **Discovery** tool. If you anonymize the data after you discover devices, the new data coming into the system is anonymized, but the existing data is not anonymized.

Step 8 Click **Save Configuration**.

Step 9 To view configured instances, click the **Instances** tab.

Step 10 To view summary information and metrics, select an instance from the list.

Step 11 (Optional) If Catalyst Center integrates with Connected Mobile Experience (CMX), you have the option of anonymizing data on the CMX side. Do these steps:

a) Using an SSH client, log in to CMX as the cmxadmin CLI user.

b) Change to the root user.

c) Go to `/opt/cmx/etc/node.conf` and under `[location]`, add **`user_options`**. For example:

```
[location]
…
user_options=-Dhideusername=true
```

d) On the CMX CLI, enter these commands:

```
cmxctl agent restart
cmxctl location restart
```

View data retention settings

You can view how long data is stored for an application.

Procedure

Step 1 From the main menu, choose **System** > **Data Platform**.

Step 2 Click **Store Settings**.

Step 3 To view a list of historical purge jobs that have completed, click **Data Purge Schedule**.

The **HISTORY** table lists the name of the purge job, the result, the time, and other data. You can sort, filter, and export data in the table.

Step 4 To view the current data retention and purge settings, click **Data Retention & Purge Configuration**.

The **Metric Graph Store** option appears. It displays settings for all time-based graphical data, such as the maximum size and the low and high watermark threshold.

View pipeline status

Data pipelines allow Catalyst Center applications to process streaming data. A data pipeline encapsulates a series of computations. It accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas.

Procedure

Step 1 From the main menu, choose **System** > **Data Platform**.

Step 2 Click **Pipelines**.

Step 3 To view whether the application is receiving data from the underlying pipelines, click a pipeline name.

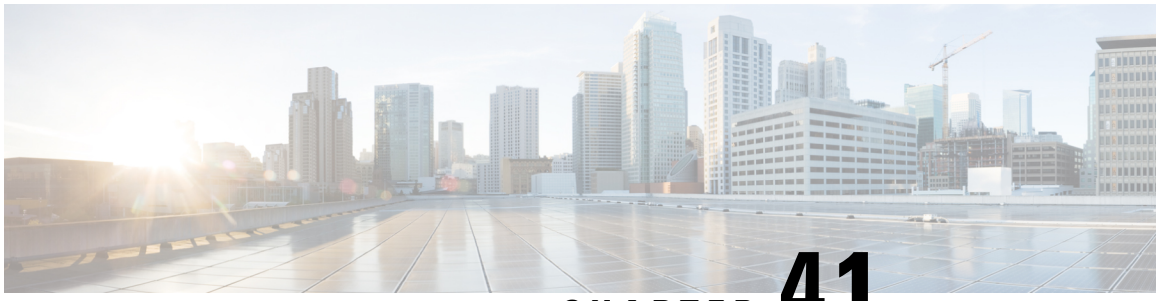
The appropriate *Pipeline* page displays with these tabs:



Note Make sure to click the **Exceptions** tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**: Displays metrics that update every 30 minutes.

- **Summary**: Displays summary information, such as statistics, runtime, and manifest.
- **Exceptions**: Displays any exceptions that have occurred on the pipeline.
- **Stages**: Displays the pipeline stages.



CHAPTER 41

Proactive Remediation for Discovered Issues

- Proactive remediation for discovered issues, on page 1471
- Approve or decline a corrective action, on page 1471

Proactive remediation for discovered issues

Catalyst Center can resolve certain discovered issues on clusters connected to Cisco DNA Connect cloud without requiring an upgrade to a newer release or package.

When a corrective action requires your approval, Catalyst Center displays an **Action Required** dialog box on the home page. The dialog box identifies the issue, explains the potential impact, and describes the recommended action. Depending on the issue, it may include a defect or reference ID.

If you approve the corrective action, Catalyst Center displays a **Remedy Applied** notification after the corrective action is complete. The notification describes the result of the corrective action.

For further assistance, contact Cisco TAC.

Examples of proactive remediation

- Restore Assurance Device 360 SNMP data collection when an issue affects the visibility of real-time device performance metrics.
- Remove stale entries that can delay or create gaps in Assurance data processing.
- Update a critical configuration setting that is required to enable release upgrades.

Approve or decline a corrective action

Use this procedure to approve or decline a corrective action for proactive remediation of discovered issues.

Before you begin

Catalyst Center must be connected to Cisco DNA Connect cloud.

Procedure

Step 1 In the **Action Required** dialog box on the home page, review the issue, potential impact, and recommended corrective action.

Step 2 Select the appropriate response in the dialog box.

Some dialog boxes also allow you to ignore the message or suppress future messages. Available options are:

Option	Description
Yes	Catalyst Center applies the validated corrective action and notifies you after completion.
No	Catalyst Center does not apply the corrective action. Contact Cisco TAC if you need assistance.
Ignore	Catalyst Center does not take any action. Depending on the issue, the dialog box may reappear.
Do not show this again	Catalyst Center suppresses the dialog box in the future.

Step 3 Click **Okay**.

If you approve the corrective action, Catalyst Center displays a **Remedy Applied** notification after the corrective action is complete.