

Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2020-05-16

Last Modified: 2025-12-19

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)

© 2019–2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **What's New in Cisco IOS XE (Catalyst SD-WAN)** 3

CHAPTER 3 **Cloud OnRamp for IaaS** 5

- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 5
- Overview 6
- Supported Cisco Cloud Service Providers and Supported Cisco Catalyst SD-WAN Cloud Devices 8
- Prerequisites of Cisco Catalyst SD-WAN Cloud Devices 8
  - Provision Cisco SD-WAN Manager Server 8
  - Verify Presence of Cisco Catalyst SD-WAN Cloud Devices in Cisco SD-WAN Manager 9
  - Configure Device Template for Cisco Catalyst SD-WAN Cloud Devices 10
  - Attach a Device Template to Cisco Catalyst SD-WAN Cloud Devices 10
- AWS Prerequisite 11
- Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS 12
- Manage Host and Transit VPCs 17
  - Display Host VPCs 17
  - Map Host VPCs to a Transit VPC 18
  - Unmap Host VPCs 18
  - Display Transit VPCs 18
  - Add Transit VPC 19
  - Delete Device Pair 19
  - Delete Transit VPC 19
  - Add Device Pairs 20
  - History of Device Pairs for Transit VPCs 21
  - Edit Transit VPC 21

Microsoft Azure Prerequisites 22
Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure 25
Manage Host and Transit VNets 29
Display Host VNets 29
Map Host VNets to an Existing Transit VNet 29
Unmap Host VNets 29
Display Transit VNets 30
Add Transit VNet 30
Delete Transit VNet 30
Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 31
Sample Feature Template Settings 34
Sample Device Template Variable Values 40
Example for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS 40

CHAPTER 4 **Cloud OnRamp for Colocation** 45
Deploy Cloud OnRamp for Colocation Solution 46
Manage Cloud OnRamp for Colocation Devices 48
Add Cloud OnRamp Colocation Devices 48
Delete Cloud OnRamp for Colocation Devices 49
Manage Clusters 50
Provision and Configure Cluster 51
Create and Activate Clusters 52
Cluster Configuration 54
Progress of Cluster Activation 63
View Cluster 66
Edit Cluster 66
Add CSP Device to Cluster 67
Delete CSP Devices from Cluster 68
Delete CSP with Cisco Colo Manager 69
Replace Cisco CSP Devices After RMA 70
Return of Materials of Cisco CSP Devices 71
RMA Process for Cisco CSP Devices 71
Prerequisites and Restrictions for Backup and Restore of CSP Devices 72
Remove Cluster 74

Reactivate Cluster 74
Manage Service Groups 75
Create Service Chain in a Service Group 75
QoS on Service Chains 81
Clone Service Groups 82
Create Custom Service Chain 84
Custom Service Chain with Shared PNF Devices 85
Custom Service Chain with Shared VNF Devices 88
View Service Groups 90
Edit Service Groups 90
Attach or Detach a Service Group in a Cluster 91
Manage VM Catalog and Repository 92
Upload VNF Images 93
Create Customized VNF Image 95
View VNF Images 100
Delete VNF Images 100
Upgrade Cisco NFVIS Using Cisco SD-WAN Manager 101
Upload NFVIS Upgrade Image 101
Upgrade a CSP Device with a Cisco NFVIS Upgrade Image 101
Supported Upgrade Scenarios and Recommended Connections 102
Monitor Operational Status of Cloud OnRamp for Colocation Devices from Cisco Catalyst SD-WAN Manager 104
View Cisco Colo Manager Health 105
View Information About VNFs 106
Monitor Cloud OnRamp Colocation Clusters 108
Packet Capture for Cloud OnRamp Colocation Clusters 112
Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Multitenancy 114
Overview of Colocation Multitenancy 114
Roles and Functionalities in a Multitenant Environment 115
Recommended Specifications in a Multitenant Environment 116
Assumptions and Restrictions in Colocation Multitenancy 116
Service Provider Functionalities 118
Provision a New Tenant 118
Delete an RBAC User from a Colocation User Group 120

Manage Tenant Colocation Clusters 120
Tenant Functionalities 121
Manage Colocation Clusters as Tenants 121
Monitor Colocation Cluster Devices and Cisco Catalyst SD-WAN Devices in Comanaged Multitenant Environment 122

PART I **Cloud OnRamp for SaaS** 123

CHAPTER 5 **Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later** 125
Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later 126
Information About Cloud OnRamp for SaaS 126
User-defined probe endpoints for applications 127
Cloud OnRamp for SaaS capable applications 127
Prerequisites for Cloud OnRamp for SaaS 127
Restrictions for Cloud OnRamp for SaaS, General 128
Restrictions for Service VPN Gateway Mode 128
Configure Cloud OnRamp for SaaS Using a Workflow 129
Add SaaS Applications Using Policy Groups 129
Deploy SaaS Applications Using Policy Groups 131
Add a user-defined endpoint to applications 131
Monitor Cloud OnRamp for SaaS 133
Migrate Older Cloud OnRamp for SaaS Path Selection 134

CHAPTER 6 **Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x** 137
Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x 137
Information About Cloud OnRamp for SaaS 140
Common Scenarios for Using Cloud onRamp for SaaS 141
Scenario 1: Cloud Access through Direct Internet Access Links 141
Scenario 2: Cloud Access through a Gateway Site 142
Scenario 3: Hybrid Approach 143
Specify Office 365 Traffic Category 144
Best path determination 144

Load Balancing Across Multiple Interfaces 144
Information About Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites 145
Information About Cloud OnRamp for SaaS Support for Webex 147
Information About the SD-AVC Cloud Connector 148
Information About Viewing Path Scores for Office 365 Traffic 149
Information About Configuring the Traffic Category and Service Area for Specific Policies 149
Benefits of Configuring the Traffic Category and Service Area for Specific Policies 149
Information About Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites 149
Benefits of Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites 150
Information About Visibility for Microsoft 365 SaaS Traffic 150
Benefits of Visibility for Microsoft 365 SaaS traffic 150
Information About Including or Excluding Microsoft Telemetry Data from the Best Path Decision for Microsoft 365 Traffic 150
Information About Cloud OnRamp for SaaS Support for Loopback, Dialer, and Subinterfaces 151
Information About Excluding Data Prefixes 151
Information About Using a Tracker for Faster Failover 151
Benefits of Cloud onRamp for SaaS 152
Benefits of Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites 152
Benefits of Cloud onRamp for SaaS Support for Webex 152
Supported Devices for Cloud onRamp for SaaS 152
Prerequisites for Cloud OnRamp for SaaS 153
Prerequisites for Cloud OnRamp for SaaS, General 153
Prerequisites for Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites 154
Prerequisites for Cloud OnRamp for SaaS Support for Webex 154
Prerequisites for Configuring the Traffic Category and Service Area for Specific Policies 154
Prerequisites for Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites 155
Prerequisites for Visibility for Microsoft 365 SaaS Traffic 155
Prerequisites for Including or Excluding Microsoft Telemetry Data from the Best Path Decision for Microsoft 365 Traffic 155
Prerequisites for Webex Server-Side Metrics 155
Prerequisites for Cloud OnRamp for SaaS Support on Loopback, Dialer, and Subinterfaces 155
Prerequisites for Excluding a Data Prefix List for a Cloud OnRamp for SaaS Application 156

Prerequisites for Faster Failover with a DIA Tracker 156
Restrictions for Cloud onRamp for SaaS 156
Restrictions for Cloud OnRamp for SaaS, General 156
Restrictions for Service VPN Gateway Mode 157
Restrictions for the Webex Application 158
Restrictions for Associating a Tracker with DIA and Gateway Sites 158
Use Cases for Cloud onRamp for SaaS 158
Use Cases for Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites 158
Use Cases for the SD-AVC Cloud Connector 158
Use Case for Configuring the Traffic Category and Service Area 159
Use Case for Enabling Specific Applications at Specific Sites 159
Use Case for Excluding Data Prefixes from Cloud OnRamp for SaaS Optimization 159
Configure Cloud onRamp for SaaS 160
Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices 160
Enable Cloud OnRamp for SaaS 160
Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager 161
Configure Sites for Cloud onRamp for SaaS Using Cisco SD-WAN Manager 164
Configure Client Sites 165
Edit Interfaces on Gateway Sites 168
Configure Direct Internet Access (DIA) Sites 170
Edit Interfaces on Direct Internet Access (DIA) Sites 171
Enable Application Feedback Metrics for Office 365 Traffic 172
Enable Microsoft to Provide Telemetry for Office 365 Traffic 173
Enable Webex for Cloud OnRamp for SaaS 174
Enable Webex Server-Side Metrics 174
Update the Webex Server Information for Cloud OnRamp for SaaS 176
Configure the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager 176
Configure AAR Policy to Enable Cloud OnRamp Operation on Specific Applications at Specific Sites Using Cisco SD-WAN Manager 177
Enable Application Visibility and Flow Visibility 178
Configure Visibility for Microsoft 365 SaaS traffic Using Cisco SD-WAN Manager 178
View Application Usage 179
Verify Cloud onRamp for SaaS 179

Verify That an Application is Enabled for Cloud OnRamp for SaaS 180
Verify Changes to the Configuration of the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager 180
Verify Which Applications Are Enabled for Specific Devices Using Cisco SD-WAN Manager 180
Verify Which Applications Are Enabled for a Specific Policy Using Cisco SD-WAN Manager 181
Verify the Excluded Data Prefixes Using Cisco SD-WAN Manager 181
Monitor Cloud onRamp for SaaS 182
View Details of Monitored Applications 182
Monitor the Status of Webex for Cloud OnRamp for SaaS 184
View Server Information Using the SD-AVC Cloud Connector 184
Monitor an Excluded Data Prefix List for Cloud OnRamp for SaaS 186
View Logs in Syslog And Console Log 186
Cloud onRamp for SaaS Over SIG Tunnels 187
Prerequisites for Cloud onRamp for SaaS Over SIG Tunnels 187
Restrictions for Cloud OnRamp for SaaS Over SIG Tunnels 187
Information About Cloud OnRamp for SaaS Over SIG Tunnels 188
Benefits of Cloud onRamp for SaaS Over SIG Tunnels 188
Use Cases for Cloud onRamp for SaaS Over SIG Tunnels 188
Configure Cloud OnRamp for SaaS Over SIG Tunnels 191
Configure Cloud onRamp for SaaS Over SIG Tunnels Using the CLI 193
Monitor Cloud OnRamp for SaaS Over SIG Tunnels 194
Monitor Cloud onRamp for SaaS Over SIG Tunnels Using the CLI 194
Configuration Example for Cloud onRamp for SaaS Over SIG Tunnels 196
Troubleshooting Cloud OnRamp for SaaS 196
Cannot Enable Telemetry for the Webex Application 196
Failing to Identify the Best Path for Each Webex Region 196
Debug and Show Commands 197

CHAPTER 7 **Application Lists** 201
Information About SaaS Application Lists 201
Benefits of SaaS Application Lists 202
Prerequisites for SaaS Application Lists 203
Restrictions for SaaS Application Lists 203
Use Cases for SaaS Application Lists 203

Workflow 205
Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager 205
View SaaS Application Lists 206

CHAPTER 8 Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r 207
Overview: How to Configure Cloud onRamp for SaaS 208
Common Scenarios for Using Cloud onRamp for SaaS 209
Scenario 1: Cloud Access through Direct Internet Access Links 209
Scenario 2: Cloud Access through a Gateway Site 211
Scenario 3: Hybrid Approach 213
Create a Probes Feature Template 214
Create a Policy for Cloud onRamp for SaaS 217

PART II Cloud OnRamp for Multicloud (Cisco IOS XE Catalyst SD-WAN Release 17.16.x and Later) 221

CHAPTER 9 Cloud OnRamp for Multicloud - Cloud and Interconnect 223
Cloud OnRamp for Multicloud 223
Prerequisites for existing Transit Gateway connectivity 224
Workflow to Configure Cloud OnRamp for Multicloud 225
Manage Accounts 226
Add an AWS Cloud Account 226
Add an Azure Cloud Account 228
Add a Google Cloud Account 229
Associate a Megaport Account 230
Associate an Equinix Account 231
Global Settings 232
Configure Global Settings for AWS 232
Configure Global Settings for Azure and Azure Gov Cloud 236
Configure Global Settings for Google Cloud 238
Configure Global Settings for Megaport 239
Configure Global Settings for Equinix 240
Add VPCs/VNets Tags 241
Create Tags for AWS 241
Create Tags for Azure and Azure Gov Cloud 242

Create Tags for Google Cloud 243
Create and Manage Gateways 243
Create and Manage Cloud Gateways 243
Create and Manage Interconnect Gateways 256
Cloud Connections 262
Configure Transit Gateway connections through AWS portal 263
Rebalance VNets 264
Interconnect Connections 264
Middle-Mile Networks 265
Multicloud Networks 280
Virtual Networks 291
View, Edit, or Delete Connections 293
Audit 294

PART III **Cloud OnRamp for Multicloud (Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Earlier)** 303

CHAPTER 10 **Cloud OnRamp for Multicloud** 305

CHAPTER 11 **AWS Integration** 307
Information about AWS Integration 308
AWS Branch Connect Overview 311
AWS Cloud WAN 312
Upgrade Considerations from Cisco Catalyst SD-WAN Manager Release 20.12.1 to Cisco Catalyst SD-WAN Manager Release 20.13.1 312
Information About Configuring Devices for AWS Integration Using Configuration Groups 313
Restrictions for AWS Integration 313
Configure AWS Integration 314
Create AWS Cloud Account 314
Configure Cloud Global Settings 317
Discover Host Private Networks 324
Create Cloud Gateway 325
Configure Site Attachment 327
Intent Management - Connectivity 328
Transit Gateway Peering 331

Audit Management 331
Monitor AWS Integration using Cisco SD-WAN Manager 335

CHAPTER 12 **Amazon GovCloud (US) Integration** 337
Information About AWS GovCloud (US) Integration 338
Benefits of AWS GovCloud (US) Integration 338
Supported Devices for AWS GovCloud (US) 339
Prerequisites for AWS GovCloud (US) Integration 339
Restrictions for AWS GovCloud (US) Integration 340
Use Case for AWS GovCloud (US) Integration 340
Configure AWS GovCloud (US) 340

CHAPTER 13 **Microsoft Azure Virtual WAN Integration** 343
Information About Azure Virtual WAN Integration 345
Azure Virtual WAN Hub Integration with Cisco Catalyst SD-WAN 345
How Virtual WAN Hub Integration Works 346
Connectivity Models 347
Routing Traffic Flow to a Secured Virtual Hub or a Local Firewall 348
Azure Virtual WAN Audit 349
Information About Periodic Audit 349
Audit Discrepancies and Resolutions 349
SKU Scale Value of Network Virtual Appliances 352
Security Rules Configuration of Network Virtual Appliances 352
Information About Azure ExpressRoute Connection to NVA 353
Information about Multiple Virtual Hubs in Each Region 353
Supported Devices for Azure Virtual WAN Integration 353
Prerequisites for Azure Virtual WAN Integration 354
Prerequisites for Routing Traffic to a Secured Virtual Hub or a Local Firewall 354
Prerequisites for Azure SKU Scaling, Audit, and Security Rules of Network Virtual Appliances 354
Restrictions for Azure Virtual WAN Integration 355
Restrictions for Azure Virtual WAN Integration 355
Restrictions for Routing Traffic to a Secured Virtual Hub or a Local Firewall 355
Restrictions for Azure SKU Scaling, Audit, and Security Rules of Network Virtual Appliances 356
Restrictions for Multiple Virtual Hub per Region 356

Use Cases for Azure Virtual WAN Integration 356
Use Cases for Routing Traffic Flow to a Secured Virtual Hub or a Local Firewall 356
Use Cases for Azure SKU Scaling 356
Use Cases for Azure Audit 356
Use Cases for Security Rules of NVAs 357
Configure Azure Virtual WAN Integration 357
Configure Azure Virtual WAN Hubs 357
Configuration Prerequisites 357
Integrate Your Azure Cloud Account 357
Create and Manage Cloud Gateways 360
Discover Host VNets and Create Tags 363
Map VNets Tags and Branch Network VPNs 364
Rebalance VNets 364
Configure an Azure Virtual WAN Hub Through the Azure Portal 365
Configure Routing of Traffic Flow to a Secured Virtual Hub or a Local Firewall 368
Route Local Outgoing Traffic Flow to an Azure Secured Virtual Hub 369
Route Azure Outgoing Traffic Flow to a Local Branch Router 369
Configure SKU Scale Value 370
Initiate On-Demand Audit 370
Enable Periodic Audit 371
Configure Security Rules of NVAs 371
Verify Azure Virtual WAN Integration 372
View, Edit, or Delete a Cloud Gateway 372
Verify Azure SKU Scale Value Update 372
Verify Security Rule for Network Virtual Appliances 373
Monitor Azure Virtual WAN Integration Using Cisco SD-WAN Manager 373
Monitor Azure Virtual WAN Integration 373

CHAPTER 14 **Microsoft Azure for US Government Integration** 375
Information About Azure for US Government Integration 376
Benefits of Azure for US Government Integration 376
Supported Devices for Azure for US Government 376
Prerequisites for Azure for US Government Integration 377
Restrictions for Azure for US Government Integration 377

Use Case for Azure for US Government Integration 377
Configure Azure for US Government 377
Monitor Azure for US Government Integration 378

CHAPTER 15 Google Cloud Integration 379
Supported Platforms and Instances 381
Limitations and Restrictions 382
Overview of Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud 383
Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway 383
Google Service Directory Integration and Lookup 384
Connectivity Models 385
Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways 386
Configure Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud 387
Configuration Prerequisites 387
Attach Cisco Catalyst 8000V Instances to a Device Template 388
Associate Your Google Cloud Account with Cisco SD-WAN Manager 389
Configure Cloud Global Settings 390
Discover Host VPCs and Create Tags 391
Create and Manage Cloud Gateways 392
Map VPC Tags and Branch Network VPNs 393
Service Directory Lookup and Traffic Policies with Discovered Apps 394
Enable Service Directory Lookup 395
Create Traffic Policies Using Cloud Discovered Apps 396
Monitor Connectivity 397
Audit 397
View Cloud Resource Inventory 399

CHAPTER 16 Cisco Catalyst SD-WAN Manager Support for Monitoring Multicloud Services 401
Restrictions for Monitoring Multicloud Services using Cisco SD-WAN Manager 401
Information about Monitoring Multicloud Services using Cisco SD-WAN Manager 402
Geographical View 402
Cloud and Interconnect Dashboard 403
Cloud Gateway Summary View 404
Interconnect Gateway Summary View 404

PART IV **Cloud OnRamp for Multicloud: Cisco Catalyst SD-WAN Cloud Interconnect (Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Earlier)** 407

CHAPTER 17 **Cloud OnRamp for Multicloud: Cisco Catalyst SD-WAN Cloud Interconnect** 409

CHAPTER 18 **License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport** 411

Information About License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 412

Interconnect Gateway Licenses 412

Interconnect Connection Licenses 414

Supplemental Licenses 416

License Enforcement 417

License Enforcement for Interconnect Gateways 417

License Enforcement for Short-Haul Interconnect Connections 418

License Enforcement for Long-Haul Interconnect Connections 419

License Enforcement for AWS Hosted Connections 420

Information About Pay As You Go License 420

View Licenses Associated with a Megaport Account 421

Find License SKU Associated with an Interconnect Gateway 423

Find License SKU Associated with an Interconnect Connection 423

CHAPTER 19 **Cisco Catalyst SD-WAN Cloud Interconnect with Megaport** 425

Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 429

Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 430

Restrictions for Encrypted Multicloud Interconnects 432

Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 433

Information About Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 436

Benefits of Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 437

Encrypted Multicloud Interconnects 438

Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 438

Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Megaport 440

Associate Megaport Account with Cisco SD-WAN Manager 440

Configure Global Settings for Interconnect Gateways 441

Attach Megaport Template to Cisco Catalyst 8000v Instance 442
Create an Interconnect Gateway at a Megaport Location 443
Create Interconnects to AWS 446
Associate AWS Account with Cisco SD-WAN Manager 446
Discover Host Private Networks and Tag AWS VPCs 446
Create Direct Connect Public Hosted VIF to AWS from Interconnect Gateway 449
Create Direct Connect Private Hosted VIF to AWS Direct Connect Gateway from Interconnect Gateway 451
Create Direct Connect Public Hosted Connection to AWS from Interconnect Gateway 454
Create Direct Connect Private Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway 456
Create Direct Connect Transit Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway 459
Create Interconnects to Google Cloud 462
Associate Google Cloud Account with Cisco SD-WAN Manager 462
Create Interconnect to Google Cloud Routers from Interconnect Gateways 463
Create Interconnect Connection to a Cloud Gateway In Google Cloud 468
Create Interconnects to Microsoft Azure 471
Associate Microsoft Azure Account with Cisco SD-WAN Manager 471
Discover Host Private Networks and Tag Microsoft Azure VNets 472
Create Microsoft-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways 475
Create Private-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways 479
Create Interconnect Between Interconnect Gateways 484
Verify and Modify Configuration 486
View Interconnect Gateway and Connection Summary 486
View, Edit, or Delete Connections 486
View, Edit, or Delete an Interconnect Gateway 491
View, Edit, or Delete an Interconnect Account 492
Audit Management 492
Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Megaport 493

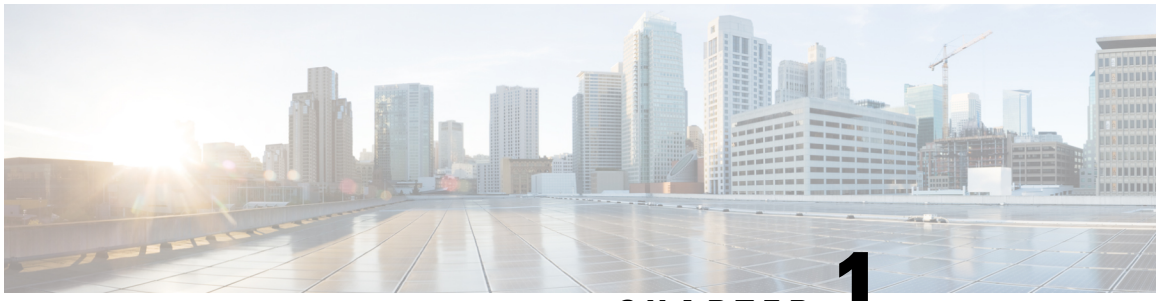
CHAPTER 20 **Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 497**
Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 499
Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 499

Restrictions for Encrypted Multicloud Interconnects 501
Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 502
Information About Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 505
Benefits of Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 507
Encrypted Multicloud Interconnects 507
Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 508
Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Equinix 510
Associate Equinix Account with Cisco SD-WAN Manager 510
Configure Global Settings for Equinix Interconnect Gateways 510
Attach Equinix Template to Cisco CSR 1000v or Cisco Catalyst 8000v Instance 512
Create Interconnect Gateway at an Equinix Location 513
Create Interconnect to AWS 515
Associate AWS Account with Cisco SD-WAN Manager 515
Discover Host Private Networks and Tag AWS VPCs 516
Create Direct Connect Public Hosted Connection to AWS from Interconnect Gateway 517
Create Direct Connect Private Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway 518
Create Direct Connect Transit Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway 521
Create Interconnects to Google Cloud 524
Associate Google Cloud Account with Cisco SD-WAN Manager 524
Create Interconnect to Google Cloud Routers from Interconnect Gateways 524
Create Interconnect Connection to a Cloud Gateway In Google Cloud 530
Create Interconnects to Microsoft Azure 533
Associate Microsoft Azure Account with Cisco SD-WAN Manager 533
Discover Host Private Networks and Tag Microsoft Azure VNets 534
Create Microsoft-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways 537
Create Private-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways 541
Device Links 545
Add Device Links 546
Delete Device Links 546
Update Device Links 547
Create Interconnect Between Interconnect Gateways 547
Verify and Modify Configuration for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 549

View Interconnect Gateway and Connection Summary 549
View, Edit or Delete Connections 550
View, Edit, or Delete an Interconnect Gateway 553
View, Edit, or Delete an Interconnect Account 553
Audit Management 554
Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Equinix 556

PART V **Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp** 559

CHAPTER 21 **Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp** 561
Overview 561
Support Articles 561
Feedback Request 562
Disclaimer and Caution 562



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

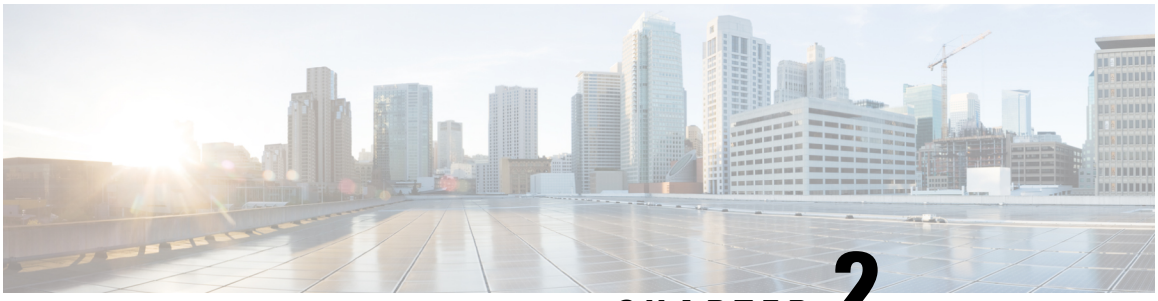
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

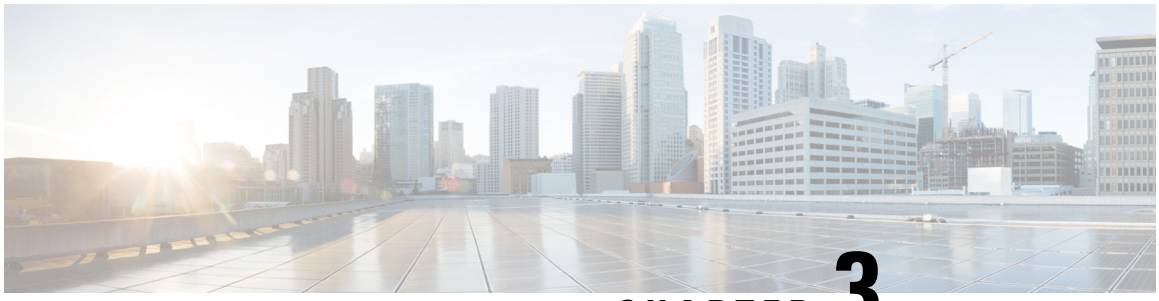


CHAPTER 2

What's New in Cisco IOS XE (Catalyst SD-WAN)

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x

What's New in Cisco SD-WAN (vEdge) Release 20.x



CHAPTER 3

Cloud OnRamp for IaaS

- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, on page 5
- Overview, on page 6
- Supported Cisco Cloud Service Providers and Supported Cisco Catalyst SD-WAN Cloud Devices, on page 8
- Prerequisites of Cisco Catalyst SD-WAN Cloud Devices, on page 8
- AWS Prerequisite, on page 11
- Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS, on page 12
- Manage Host and Transit VPCs, on page 17
- Microsoft Azure Prerequisites, on page 22
- Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure, on page 25
- Manage Host and Transit VNets, on page 29
- Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, on page 31
- Sample Feature Template Settings , on page 34
- Sample Device Template Variable Values, on page 40
- Example for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, on page 40

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

Table 1: Feature History

Feature Name	Release Information	Description
Azure Government Cloud Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to configure the Cisco Catalyst 8000V devices on Microsoft Azure Government Cloud. With these cloud devices now supported on Microsoft Azure Government Cloud, Government Cloud customers can use the same advanced routing and security benefits, which are already available on Azure public cloud.

Feature Name	Release Information	Description
AWS Government Cloud Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to configure Cisco CSR1000V on Amazon Web Services (AWS) Government Cloud. With Cisco CSR1000V now supported on AWS Government Cloud, Government Cloud customers can move sensitive workloads into the cloud and manage the data securely by using all routing benefits.
	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	Starting from this release, Cisco Catalyst 8000V devices are supported on AWS Government Cloud.

Overview

Note Beginning with Cisco vManage Release 20.9.1, we recommend setting up your cloud infrastructure using Cloud OnRamp for Multicloud. Cloud OnRamp for IaaS will be phased out in a future release.

Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) extends the fabric of Cisco Catalyst SD-WAN overlay network to public cloud instances. Cisco Catalyst SD-WAN Cloud OnRamp for IaaS allows branches with Cisco Cloud Services Router 1000V Series and Cisco Catalyst 8000V devices to connect directly to public-cloud application providers. By eliminating the need for a physical data center, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS improves the performance of SaaS applications.

To know more about Cisco Catalyst 8000V devices, see the Cisco Catalyst 8000V Edge Software Configuration Guide.

The connection between the overlay network and a public-cloud application is provided by one to four pairs of redundant Cisco Catalyst SD-WAN cloud devices. These devices act together as a transit between the overlay network and an application. By using redundant devices to form the transit, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS offers path resiliency to the public cloud. In addition, having redundant routers helps in brownout protection to improve the availability of public-cloud applications. Together, the two routers can remediate link degradation that might occur during brownouts. You can configure these devices as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow.

With Cisco Catalyst SD-WAN Cloud OnRamp for IaaS support on Amazon Web Services (AWS) and Microsoft Azure government cloud (GovCloud), you can configure Cisco CSR1000V and Cisco Catalyst 8000V devices to host sensitive data. AWS or Microsoft Azure GovCloud (US) are isolated AWS or Azure regions that allow the U.S. government agencies and customers to move sensitive workloads into the government cloud. The customers can use these devices that provide routing capabilities and support full path encryption with powerful cipher suites. The regions that you can choose during Cisco Catalyst SD-WAN Cloud OnRamp for IaaS configuration are related to the AWS or Microsoft Azure GovCloud specifications. See AWS GovCloud documentation and Microsoft Azure GovCloud documentation for details on setting up your GovCloud (US) account.

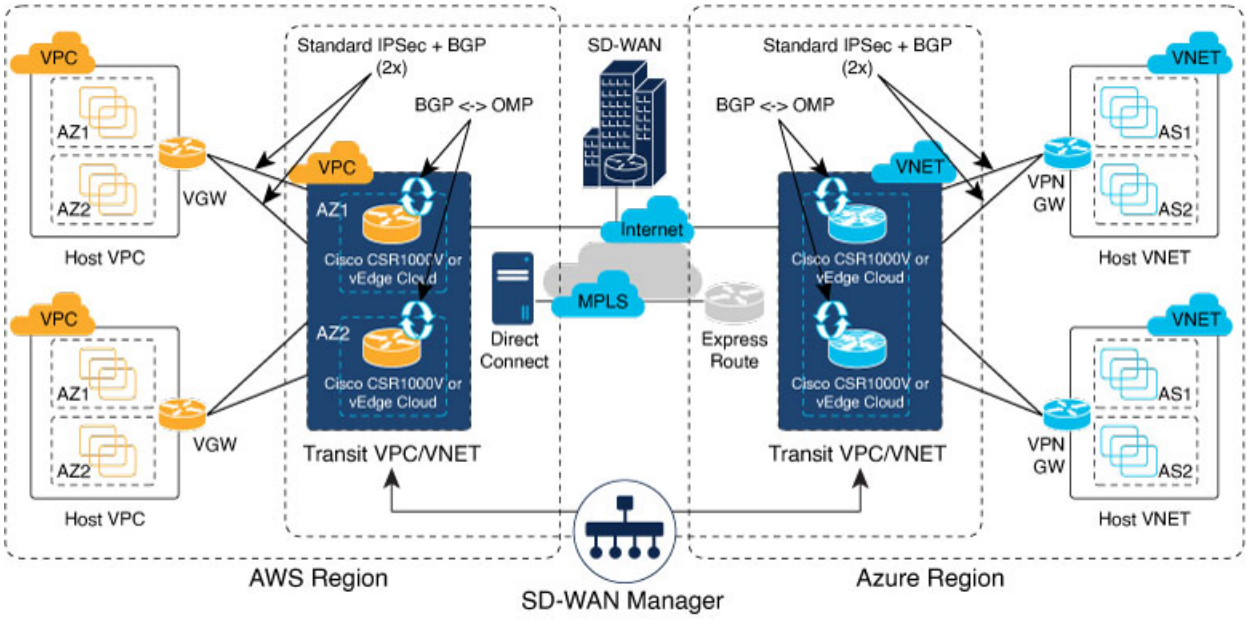
The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS works along with AWS Virtual Private Cloud (VPC) and Azure Virtual Network (VNet).

The key steps to deploy a Cisco Catalyst SD-WAN Cloud OnRamp for IaaS solution are:

1. Identify one to four pairs of unused Cisco Catalyst SD-WAN cloud devices in Cisco SD-WAN Manager that you can use forCisco Catalyst SD-WAN Cloud OnRamp for IaaS.
2. Configure and attach a basic device template to both the Cisco Catalyst SD-WAN cloud devices.
3. Enter AWS or Azure API credentials (access key and secret key) when configuring using Cisco SD-WAN Manager.
4. Add the transit Virtual Private Cloud (VPC) or transit Virtual Network (VNet) configuration.
5. Discover and map host VPCs or host VNets to the transit VPC or transit VNet.

The following image shows the topology of Cisco Catalyst SD-WAN Cloud OnRamp for IaaSwith AWS and Microsoft Azure integrated. You can apply the same policy, security, and other Cisco Catalyst SD-WAN policies everywhere with Cisco SD-WAN Manager as a single server for all the Cisco Catalyst SD-WAN devices, which are on-premises and on multiple clouds. The infrastructure on AWS and Microsoft Azure can be seamlessly integrated into the Cisco Catalyst SD-WAN fabric. The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow automates all steps, and the Cisco SD-WAN Manager server builds the whole solution within minutes.

Figure 1: Cisco Catalyst SD-WAN Cloud OnRamp for IaaS Topology



Supported Cisco Cloud Service Providers and Supported Cisco Catalyst SD-WAN Cloud Devices

The following IaaS public cloud providers are supported with Cisco Catalyst SD-WAN Cloud OnRamp for IaaS:

- Amazon AWS
- Microsoft Azure

The following devices are supported:

- Cisco Cloud Services Router 1000V Series (Cisco CSR1000V)
- Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V)



Note From Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco Catalyst 8000V replaces Cisco CSR1000V. Therefore, Azure Government Cloud support is only available for Cisco Catalyst 8000V, and we recommend that you use Cisco Catalyst 8000V devices.

In this document, the supported devices are collectively referred to as Cisco Catalyst SD-WAN cloud devices.

Prerequisites of Cisco Catalyst SD-WAN Cloud Devices

Before you can configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, ensure that the following device requirements are met.

- Verify you have available tokens or licenses for at least two Cisco CSR1000V or Cisco Catalyst 8000V devices in Cisco SD-WAN Manager. See Verify Presence of Cisco Catalyst SD-WAN Cloud Devices in Cisco SD-WAN Manager, on page 9.
- Configure feature and device templates for the Cisco CSR1000V or Cisco Catalyst 8000V devices that you'll use within the transit VPCs or VNets during configuration. See Configure Device Template for Cisco Catalyst SD-WAN Cloud Devices, on page 10.
- Attach the device template to the software tokens representing the Cisco CSR1000V or Cisco Catalyst 8000V devices that you'll use within the transit VPCs or VNets. See Attach a Device Template to Cisco Catalyst SD-WAN Cloud Devices, on page 10.

Provision Cisco SD-WAN Manager Server

Before you can configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, provision the Cisco SD-WAN Manager server.

1. Ensure that your Cisco SD-WAN Manager server can access the Internet, and you configure the DNS server so that it can reach AWS or Microsoft Azure. To configure a DNS server, in the Cisco SD-WAN

Manager VPN feature configuration template, enter the IP address of a DNS server. Next, reattach the configuration template to the VPN feature using Cisco SD-WAN Manager.

2. Ensure that you add at least two Cisco Catalyst SD-WAN cloud devices to the Cisco SD-WAN Manager server to bring up Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. Attach these two Cisco Catalyst SD-WAN cloud devices to the appropriate configuration template. Ensure that the configuration for these devices include the following attributes:
   - Hostname
   - IP address of Cisco Catalyst SD-WAN Validator
   - Site ID
   - Organization name
   - Tunnel interface configuration on the eth1 interface

     In Cisco CSR1000V or Cisco Catalyst 8000V devices, the tunnel interface is on the GigabitEthernet2 interface.

3. Ensure that you synchronize the Cisco SD-WAN Manager server with the current time. To check the current time, click the **Help (?)** icon at the top bar of the Cisco SD-WAN Manager screen. The **Timestamp** field shows the current time. If the time isn't correct, configure the Cisco SD-WAN Manager server time to point to an NTP time server, such as the Google NTP server. To configure the server time, in the Cisco SD-WAN Manager NTP feature configuration template, enter the hostname of an NTP server. Next, reattach the configuration template to the NTP feature using Cisco SD-WAN Manager. The Google NTP servers are time.google.com, time2.google.com, time3.google.com, and time4.google.com, and so on.

Verify Presence of Cisco Catalyst SD-WAN Cloud Devices in Cisco SD-WAN Manager

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 On the Device listing page, verify that there are at least two valid Cisco CSR1000V or Cisco Catalyst 8000V devices, which aren't used already.

The valid unused devices are:

- The devices that have the word, "valid"under the **Validity** column.
- The devices that have the **Assigned Template**, **Device Status**, **Hostname**, **System IP**, and **Site ID** columns blank.

Go to software.cisco.com, and use the Plug and Play Connect portal to add tokens or licenses if you have insufficient Cisco CSR1000V or Cisco Catalyst 8000V devices.

Configure Device Template for Cisco Catalyst SD-WAN Cloud Devices

Ensure that you have at least a minimal device template assigned within Cisco SD-WAN Manager to the two Cisco CSR1000V or Cisco Catalyst 8000V devices. A minimal device template is the one that uses factory default feature templates within the device template. You need at least one service VPN and the management (VPN 512) interface configured within the device template. However, we recommend that you configure a fully functional device template that includes settings specific to your deployment within custom feature templates. See Configure the Cisco SD-WAN Routers for step-by-step instructions on how to create individual feature templates and device templates using Cisco SD-WAN Manager.

Ensure that you don't modify the feature templates after these templates have been attached to the device templates and configured using the Cloud onRamp for IaaS. The Cloud onRamp for IaaS configuration overwrites these feature templates configuration that is modified.

A sample device template, and the various feature templates which make up the device template, is available in Sample Feature Template Settings topic that you can use for Cisco CSR1000V or Cisco Catalyst 8000V devices.

Attach a Device Template to Cisco Catalyst SD-WAN Cloud Devices

When you attach a device template to the Cisco CSR1000V or Cisco Catalyst 8000V devices, Cisco SD-WAN Manager builds the configurations based on the feature templates and then saves the configurations to the designated , Cisco CSR1000V or Cisco Catalyst 8000V devices. Before you can build and save the configurations, define all variables within the feature templates attached to the device template.

To enter values of the variables manually using Cisco SD-WAN Manager, instead of uploading a .csv file:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

Note
In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

Step 2 For the desired device template, click **…** and choose **Attach Devices**.

A pop-up window listing the available devices to be attached to this configuration appear. The list of available devices contains either:

- The hostname and IP address of a device if it’s known using Cisco SD-WAN Manager.
- The chassis serial number of the devices that aren't available on the network and aren’t known to Cisco SD-WAN Manager.

Cisco CSR1000V or Cisco Catalyst 8000V devices are assigned a chassis serial number although there’s no physical chassis. The list contains only the device model that was defined when the device template was created.

Step 3 To apply the configuration template, choose one or more devices from **Available Devices** and move them to **Selected Devices**.

Note
In this document, we’re using two Cisco Catalyst SD-WAN cloud devices on which you apply the configurations.

Step 4 Click **Attach**.

The window that appears, lists the Cisco Catalyst SD-WAN cloud devices that you had chosen.

Step 5 For the first Cisco CSR1000V or Cisco Catalyst 8000V devices, click **…** and choose **Edit Device Template**.

A pop-up window appears with a list of variables and empty text boxes. There can be variables with check boxes to check and uncheck for on and off values. Make sure that you fill all text boxes. You can use the sample information available in the Sample Device Template Variable Values, on page 40 topic to fill in the variable values.

Step 6 Click **Update**.

Step 7 Repeat Steps 5–6 for the second Cisco CSR1000V or Cisco Catalyst 8000V devices.

You can download the variable values into the .csv file for future use.

Step 8 Click **Next**.

The window indicates that the configure action is applied to the two devices, which are attached to one device template.

You can select a device from the left pane to view the configuration that is saved on the Cisco Catalyst SD-WAN cloud device.

Step 9 Click **Configure Devices**.

Step 10 In the pop-up window that appears, check **Confirm configuration changes on 2 devices**.

Step 11 Click **OK**.

The **Task View** window appears.

After some time, the status of the two Cisco CSR1000V or Cisco Catalyst 8000V devices appears as **Done – Scheduled** with a message indicating that the device is offline and that the template will be attached to the device when it's online.

What to do next

You can now deploy the two Cisco CSR1000V or Cisco Catalyst 8000V devices within the AWS transit VPC or Azure transit VNet using Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

AWS Prerequisite

Procedure

Step 1 Have a valid AWS account.

Step 2 Have a valid AWS Government account for GovCloud access.

Step 3 Subscribe to the Cisco CSR1000V, Cisco Catalyst 8000V devices Amazon machine image (AMI) in your account within the AWS Marketplace. To subscribe to Amazon machine image (AMI) in your account within the AWS Marketplace:

a) Log in to Amazon Web Services Marketplace.

b) Search AWS Marketplace for: "Cisco CSR1000V or Cisco Catalyst 8000V devices".

A list of AMIs appears.

c) From the list, click the Cisco CSR1000V or Cisco Catalyst 8000V devices link that you're planning to deploy.

The subscription screen appears where you can subscribe to the Cisco CSR1000V or Cisco Catalyst 8000V devices AMI.

d) Click **Continue to Subscribe**.

e) Click **Accept Terms**.

After a few moments, a message appears that you're subscribed to use the Cisco CSR1000V or Cisco Catalyst 8000V devices AMI.

Note
Don't click **Continue to Configuration**, because Cisco Catalyst SD-WAN Cloud OnRamp for IaaS automatically configures the Cisco Catalyst SD-WAN cloud devices when it creates the transit VPC.

f) Log out of from the AWS Marketplace.

Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS

Points to Consider

- Transit VPCs provide the connection between the Cisco overlay network and the cloud-based applications running on host VPCs. You can provision up to four pairs of redundant Cisco Catalyst SD-WAN cloud devices within each VPC dedicated to function as a transit point for traffic from the branch to host VPCs. The individual Cisco Catalyst SD-WAN devices of each redundant pair are deployed within a different availability zone in the AWS region of the transit VPC. Multiple Cisco Catalyst SD-WAN devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two Cisco Catalyst SD-WAN cloud devices, the transport VPN (VPN 0) connects to a branch router, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VPCs to a transit VPC. To add the public IP address of the WAN interface, configure the VPN interface ethernet template with GigabitEthernet2 interface for the devices used in Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. In Cisco CSR1000V and Cisco Catalyst 8000V devices, the tunnel interface is on the GigabitEthernet2 interface. See sample VPN interface ethernet template configuration in VPN0 Interface Feature Template, on page 37.
- Cisco Catalyst SD-WAN Cloud OnRamp for IaaS supports autoscale for AWS. To use the AWS autoscale feature, ensure that you associate one to four pairs of Cisco Catalyst SD-WAN cloud devices with a transit VPC.
- Host VPCs are virtual private clouds in which your cloud-based applications reside. When a transit VPC connects to an application or application provider, it's simply connecting to a host VPC.
- All host VPCs can belong to the same AWS account, or each host VPC can belong to a different account. You can map a host that belongs to one AWS account to a transit VPC that belongs to a different account. You configure cloud instances or cloud accounts by using the Cloud OnRamp configuration wizard.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for IaaS**.

If you're configuring Cisco Catalyst SD-WAN Cloud OnRamp for IaaS the first time, no cloud instances appear in the screen. A cloud instance corresponds to an AWS account with one or more transit VPCs created within an AWS region.

Step 2 Click **Add New Cloud Instance**.

Step 3 Click the **Amazon Web Services (AWS)** radio button.

Step 4 In the next pop-up window, perform the following:

a) To log in to the cloud server, click **IAM Role** or **Key**. We recommend that you use IAM Role.

b) If you click **IAM Role**, then create an IAM role with Cisco SD-WAN Manager provided **External ID**. Note the displayed external Id from the window and provide the **Role ARN** value that is available when creating an IAM role.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, to create an IAM role, you must enter the Cisco SD-WAN Manager provided External Id into a policy by using the AWS Management Console. Do the following:

1. Attach an IAM Role to an existing Cisco SD-WAN Manager EC2 instance.

   a. See the Creating an IAM role (console) topic of AWS documentation to create a policy. In the AWS **Create policy** wizard, click **JSON** and enter the following JSON policy document.

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

   b. See the Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console blog of AWS Security Blog for information about creating an IAM role and attaching it to the Cisco SD-WAN Manager EC2 instance based on the policy created in Step 1.

   Note
   On the **Attach permissions policy** window, choose the AWS-managed policy that you created in Step 1.

2. Create an IAM role on an AWS account that you want to use for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

   a. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 4(b).

b. See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

In the **IAM Roles** window, scroll down and click the role you created in the previous step.

In the **Summary** window, note the **Role ARN**.

Note
You can enter this role ARN value when you choose the IAM role in Step 4(b).

c. After modifying the trust relationship, click **JSON** and enter the following JSON document. Save the changes.

Note
The account Id in the following JSON document is the Cisco SD-WAN Manager EC2 instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
       }
      }
    }
  ]
}
```

c) If you click the **Key** radio button:

1. In the **API Key** field, enter your Amazon API key.
2. In the **Secret Key** field, enter the password associated with the API key.
3. From the **Environment** drop-down list, choose **commercial** or **govcloud**.

   By default, commercial environment is selected. You can choose the geographical regions based on the environment specifications.

Step 5 Click **Login** to log in to the cloud server.

The cloud instance configuration wizard appears. This wizard consists of three screens that you use to select a region, add a transit VPC, discover host VPCs, and map host VPCs to transit the VPC. A graphic on each wizard screen illustrates the steps in the cloud instance configuration process. The steps that aren't yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

Step 6 Select a region:

From the **Choose Region** drop-down list, choose a region where you want to create the transit VPC.

Step 7 Add a transit VPC:

a) In the **Transit VPC Name** field, enter the transit VPC name.

The name can contain 128 alphanumeric characters, hyphens (–), and underscores (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VPC:

1. In the **WAN Edge Version** drop-down list, choose the software version of the Cisco Catalyst SD-WAN cloud device to run on the transit VPC.
2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of the Cisco Catalyst SD-WAN cloud devices that run on the transit VPC.
   - See the Supported Instance Types topic for Cisco CSR1000V devices of the *Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services*.
   - See the Supported Instance Types topic for Cisco Catalyst 8000V in the *Deploying Cisco Catalyst 8000V on Amazon Web Services*.

   Note
   We recommend that you choose the following size:

   For Cisco CSR1000V and Cisco Catalyst 8000V, choose c5 instance type with four or more than four vCPUs, such as c5.xlarge (4 vCPU).
3. In the **Max. Host VPCs per Device Pair** field, select the maximum number of host VPCs that can be mapped to each device pair for the transit VPC. Valid values are 1–32.
4. To set up the transit VPC devices for Direct Internet Access (DIA), click one of the following:
   - **Disabled**: No Internet access.
   - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.
   - **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.
5. In the **Device Pair 1#** field, choose the serial numbers of each device in the pair. To remove a device serial number, click **X** that appears in the field.

   The serial numbers of the devices that appear are associated with a configuration template and supports the Cisco Catalyst SD-WAN WAN edge version that you selected in Step 1.
6. To add more device pairs, click .

   To remove a device pair, click .

   A transit VPC can be associated with one to four device pairs. To enable the autoscale feature on AWS, associate at least two device pairs with the transit VPC.
7. Click **Advanced**, if you wish to enter more specific configuration options:
   a. In the **Transit VPC CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16. There must be sufficient address space to create six subnets within the CIDR block.
   b. (Optional) In the **SSH PEM Key** drop-down list, choose a PEM key pair to log into an instance. The key pairs are region-specific. See the AWS Documentation for instructions about creating key pairs.

8. To complete the transit VPC configuration, click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

   With this cloud instance, a single transit VPC with two Cisco Catalyst SD-WAN cloud devices has been created. You can configure multiple transit VPCs within a single cloud instance (AWS account within a region). When multiple transit VPCs exist within a cloud instance, you can map host VPCs to any one of the transit VPCs.

9. Discover host VPCs:

   a. In the **Select an account to discover** field, choose the AWS account from which you wish to discover host VPCs.

      Alternatively, to add a new AWS account from which you wish to discover host VPCs, click **New Account**.

   b. Click **Discover Host VPCs**.

      A table appears that display the VPCs, which are available to be mapped to a transit VPC. Only the host VPCs in the selected AWS account and within the same AWS region as the transit VPC appears.

   c. In the table that appears, check one or more hosts to map to the transit VPC.

      To filter the search results, use the Filter option in the search bar and display only host VPCs that match specific search criteria.

      Click the **Refresh** icon to update the table with current information.

      Click the **Show Table Columns** icon to specify which columns to be displayed in the table.

10. Map the host VPCs to a transit VPC:

    a. In the table with all host VPCs, choose the desired host VPCs.

    b. Click **Map VPCs**. The Map Host VPCs pop-up opens.

    c. In the **Transit VPC** drop-down list, choose the transit VPC to map to the host VPCs.

    d. In the **VPN** drop-down list, choose a service VPN in the overlay network in which to place the mapping.

    e. Enable the **Route Propagation** option if Cisco SD-WAN Manager automatically propagates route to the host VPC routes table.

       By default, **Route Propagation** is disabled.

    f. Click **Map VPCs**.

After a few minutes, the **Task View** screen appears, confirming that the host VPC has been mapped to the transit VPC.

Note
When configuring the VPN feature template for VPN 0 for the two Cisco Catalyst SD-WAN cloud devices that form the transit VPC, ensure that the color you assign to the tunnel interface is a public color, and not a private color. The following are the public colors:

- **3g**
- **biz-internet**
- **blue**
- **bronze**

- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

Manage Host and Transit VPCs

Display Host VPCs

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

By default, the **Mapped Host VPCs** field is selected, and the table under mapped host VPCs list the mapped host and transit VPCs, the state of the transit VPC, and the VPN ID.

Step 2 To list unmapped host VPCs, click **Un-Mapped Host VPCs**. Then, click **Discover Host VPCs**.

Step 3 To display the transit VPCs, click **Transit VPCs**.

Map Host VPCs to a Transit VPC

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.
Step 2 Click **Un-Mapped Host VPCs**.
Step 3 In the **Select an account to discover** field, choose the AWS account from which you wish to discover host VPCs.
Step 4 Click **Discover Host VPCs**.
Step 5 From the list of discovered host VPCs, choose the desired host VPCs.
Step 6 Click **Map VPCs**. The **Map Host VPCs** pop-up opens.
Step 7 From the **Transit VPC** drop-down list, choose the desired transit VPC.
Step 8 From the **VPN** drop-down list, choose the VPN in the overlay network in which to place the mapping.
Step 9 Click **Map VPCs**.

Unmap Host VPCs

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.
Step 2 Click **Mapped Host VPCs**.
Step 3 From the list of VPCs, choose the desired host VPC that you wish to unmap.
Step 4 Click **Un-Map VPCs**.
Step 5 Click **OK** to confirm the unmapping.

Unmapping host VPCs deletes all VPN connections to the VPN gateway in the host VPC, and then deletes the VPN gateway. When you make more VPN connections to a mapped host VPC, these connections are terminated as part of the unmapping process.

Display Transit VPCs

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

Step 2 Click **Transit VPCs**.

Add Transit VPC

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

Step 2 Click **Transit VPCs**.

Step 3 Click **Add Transit VPC**.

To add a transit VPC, follow the instructions in Step 7 of Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS, on page 12.

Delete Device Pair

Note To delete the last pair of online device pairs, ensure to delete a transit VPC.

Before you begin

The device pair to be deleted should be offline.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**.

Step 2 Click a device pair ID.

Step 3 Verify that the status of the device pair is offline.

Step 4 To descale the device pairs, click the trash can icon under the **Action** column, or click **Trigger Autoscale**.

Delete Transit VPC

Note To delete the last pair of online device pairs, you should delete a transit VPC.

Before you begin

Delete the device pairs that are associated with the transit VPC.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

Step 2 Click **Host VPCs**.

Step 3 Choose all host VPCs, and click **Un-Map VPCs**.

Ensure that all host VPCs mapped with the transit VPCs are unmapped.

Step 4 Click **OK** to confirm the unmapping.

Step 5 Click **Transit VPCs**.

Step 6 For the desired transit VPC to be deleted, click the trash icon.

Note
The trash icon isn't available for the last device pair of transit VPC. Therefore, to delete the last device pair, click the **Delete Transit** drop-down list item. The trash icon is only available from the second device pair onwards.

Step 7 Click **OK** to confirm.

Add Device Pairs

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

Step 2 Click **Transit VPCs**.

A table with the list of transit VPCs appears.

Step 3 For the desired transit VPC, click **...** and choose **Add Device Pair**.

Step 4 In the **Add Device Pairs** dialog box, click **Add** to add more device pairs.

Note
Ensure that the devices you're adding are already associated with a device template.

You can add up to a total of four device pairs to the transit VPC.

Step 5 Click **Save**.

History of Device Pairs for Transit VPCs

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

Step 2 Click **Transit VPCs**.

A table with the list of transit VPCs appears.

Step 3 For the desired transit VPC, click **...** and choose **History for a device pair**.

This displays the Transit VPC Connection History page with all the corresponding events.

Step 4 View a histogram of events that occurred in the previous one hour and a table of all events for the transit VPC that you've chosen. The table lists all the events generated in the transit VPC. The events can be one of the following:

- Device Pair Added
- Device Pair Spun Up
- Device Pair Spun Down
- Device Pair Removed
- Host Vpc Mapped
- Host Vpc Unmapped
- Host Vpc Moved
- Transit Vpc Created
- Transit Vpc Removed

Edit Transit VPC

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VPC. The **Host VPCs/Transit VPCs** window opens.

Step 2 Click **Transit VPCs**.

A table with the list of transit VPCs appears.

Step 3 For the desired transit VPC, click **...** and choose, and click **Edit Transit Details**.

Step 4 To enter DIA information, follow the instructions in Step 7 (iv) of Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on AWS, on page 12.

This operation might trigger autoscale, if required.

Microsoft Azure Prerequisites

1. Have a valid Microsoft Azure account.
2. Have a valid Azure Government account for GovCloud access.

Note Azure Government Cloud support is only available for Cisco Catalyst 8000V.

3. Accept the terms and conditions for the Cisco CSR1000V or Cisco Catalyst 8000V devices in the Azure Marketplace.

   To use a Cisco Catalyst SD-WAN cloud router as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow, you must accept marketplace terms for using a virtual machine (VM). You can accept the Azure Terms of Service in one of the following ways:

   - Bring up the cloud device on the portal manually, and accept the terms as part of the final page of the onboarding wizard.
   - In the Azure APIs or on the Powershell/Cloud Shell scripts, use the Set-AzureRmMarketplaceTerms command.

4. Create an App Registration in Microsoft Azure and retrieve the credentials for your Azure account. For Cisco Catalyst SD-WAN Cloud OnRamp for IaaS, these credentials are used to authenticate the Cisco SD-WAN Manager server with Azure and bring up the VNet and the Virtual Machine instances.

   To create and retrieve Azure credentials, create an App Registration in Azure with Owner privileges:

   a. Launch the Microsoft Azure Portal.

   b. Verify Azure Active Directory (AD) Permissions. Select Azure Active Directory, and note your role. Only roles with admin privileges can register applications in your Azure AD tenant.

   c. Verify subscription permissions.

      After verifying your role and privileges associated with the Azure AD, ensure that your Azure subscription account has **Microsoft.Authorization/*/Write** access to assign a role to an Azure AD application. This access is associated only with the Owner role or User Access Administrator role.

      1. On the Azure portal, click **Subscriptions**.
      2. Navigate to a **Subscriptions** service, and click the **More Actions** icon to the right of the row.

         The **Microsoft Azure Enterprise** page appears.
      3. Choose **My permissions**. Then, click **Click here to view complete access details for this subscription**.
      4. Click **View my access** to view your assigned roles.
      5. Determine if you have adequate permissions to assign a role to an AD application. If not, ask your Azure subscription administrator to add you to **User Access Administrator** role.

d. Create an application ID and service principal:

1. In the left pane of the Azure portal, click **Azure Active Directory**.
2. From the sub-menu, click **App registrations**.
3. Click **New registration**. The system displays the **Register an application** screen.
4. In the **Name** field, enter a descriptive name such as, CloudOnRampApp.
5. In **Suported account types**, choose **Accounts in this organizational directory only (Microsoft only - Single tenant)**.
6. Under **Redirect URI**, choose **Web** for the type of application you want to create.
7. After setting the values, click **Register**.

You've now created your Azure AD application and service principal.

e. Create a secret key for the Cloud OnRamp application:

1. From **App registrations** in Azure AD, click your application.
2. On the left pane, click **Certificates & secrets**.
3. Under **Client secrets**, click **New client secret**.
4. Provide a description of the secret key, and an expiry time period for the secret key.
5. Click **Add**.

After saving the client secret, the value of the client secret or key value appears. Note this value because you can't retrieve the key later, if required. You need to provide the key value with the application ID to sign into the application you have created.

f. Get Subscription ID:

1. On the Azure portal, click **Subscriptions**.
2. Navigate to a **Subscriptions** service, and click the **More Actions** icon to the right of the row.

   The **Microsoft Azure Enterprise** page appears.
3. From the page, note the **Subscription ID**.

   You need the Subscription ID to provide Cisco SD-WAN Manager with programmatic access to your Azure Subscription.

If you have multiple subscriptions, copy and save the subscription ID which you're planning to use for configuring the CloudOnRampApp.

g. View the Tenant ID:

1. On the left pane of the Azure portal, click **Azure Active Directory**.
2. From the left pane, click **Properties**. The system displays the directory ID which is equivalent to the tenant ID.

h. Assign the Owner role to the application:

In this guide, we've provided the steps for assigning the Owner role, which lets you access and manage everything.



Note To know an appropriate role for an application, contact your Azure administrator.

1. On the left pane of the Azure portal, click **Subscriptions**.
2. Click the subscription to assign to the Cloud OnRamp application.
3. In the subscription pane, navigate to Access Control (IAM).
4. Click **Add a role assignment**. The **Add role assignment** pop-up appears.
5. From the **Role** drop-down list, choose **Owner**.
6. In the **Assign Access To** drop-down list, choose the default value, **Azure AD user**, **group**, or **service principal**.
7. From the **Select** drop-down list, choose the Cloud OnRamp application that you created in Step d.
8. Click **Save**.

You can see your application in the list of users with a role for that scope.

You can now log into the Cloud OnRamp application with the Azure credentials you created and saved.

5. Check the Azure limits associated with your account by going to your subscription in the Azure portal. Under **Settings**, choose **Usage + Quotas**.
   a. Choose a provider from the **All Providers** drop-down list.
   b. Check **Microsoft.Network**.

   You can view the amount of available availability sets for this subscription. Ensure that availability sets are sufficient that allows you to create the following resources in your account:

   - One VNet, which is required for creating the transit VNet.
   - One availability set required for Virtual Machine distribution in the transit VNet.
   - Six Static Public IP addresses associated with the transit cloud routers.
   - One Azure Virtual Network transit and two Static Public IP Addresses for each host VNet
   - Four VPN connections for mapping each host VNet



Note F-Series Azure VMs (F4 and F8) are supported on the Cisco Catalyst SD-WAN cloud devices.

Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure

In the configuration process, map one or more host VNets to a single transit VNet. When mapping, you're configuring the cloud-based applications that branch users can access.

The mapping process establishes IPsec and BGP connections between the transit VNet and each host VNet. The IPsec tunnel that connects the transit and host VNet runs IKE to provide security for the connection. For Azure, the IPsec tunnel uses IKE version 2. The BGP connection that is established over the secure IPsec tunnel allows the transit and host VNet to exchange routes. The BGP connections or the BGP routes are then re-distributed into OMP within the Cisco Catalyst SD-WAN cloud devices, which then advertises the OMP routes to the Cisco SD-WAN Controller in the domain. The transit VNet can then direct traffic from the branch to the proper host VNet and to the proper cloud-based application.

During the mapping process, the IPsec tunnels and BGP peering sessions are configured and established automatically. After establishing the mappings, you can view the IPsec and BGP configurations in the VPN Interface IPsec and BGP feature configuration templates, and modify them as necessary.

Points to Consider:

To configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Azure, create Azure transit VNets, each of which consist of a pair of routers. Then, map the host VNets to transit VNets that exist in the Azure cloud. All VNets reside in the same resource group.

- Transit VNets provide the connection between the overlay network and the cloud-based applications running on the host VNet. Each transit VNet consists of two cloud devices that reside in their own VNet. Two cloud devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two cloud devices, the transport VPN (VPN 0) connects to the simulated branch device, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VNets to a transit VNet. To add the public IP address of the WAN interface, configure the VPN Interface Ethernet template with GigabitEthernet2 interface for the devices used in Cisco Catalyst SD-WAN Cloud OnRamp for IaaS. In Cisco CSR1000V and Cisco Catalyst 8000V, the tunnel interface is on the GigabitEthernet2 interface. See sample VPN Interface Ethernet template configuration in VPN0 Interface Feature Template, on page 37.
- Host VNets are virtual private clouds in which your cloud-based applications reside. When a transit VNet connects to an application or application provider, it's simply connecting to a host VNet.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for IaaS**.

Step 2 Click **Add New Cloud Instance**

Step 3 Click the **Microsoft Azure** radio button.

Step 4 In the next pop-up screen, perform the following:

a) In the **Subscription ID** field, enter the ID of the Microsoft Azure subscription you want to use as part of the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS workflow.
b) In the **Client ID** field, enter the ID of an existing application or create a new application. To create an application, go to your **Azure Active Directory** > **App Registrations** > **New registration**. See Microsoft Azure documentation for more information on creating an application.
c) In the **Tenant ID** field, enter the ID of your account. To find the tenant ID, go to your Microsoft Azure Active Directory and click **Properties**.
d) In the **Secret Key** field, enter the password associated with the client ID.
e) In the **Environment** field, choose **commercial** or **GovCloud**.

   By default, commercial environment is selected. You can choose the geographical locations based on the environment specifications.

f) Click **Login**.

The cloud instance configuration wizard opens.

The wizard consists of three screens that you use to select a location, add a transit VNet, discover host VNets, and map host VNets to the transit VNet. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. The steps not yet completed are shown in light gray. The current step is highlighted within a blue box. All completed steps are indicated with a green checkmark and are shown in light orange.

Step 5 From the **Choose Location** drop-down list, choose a location where you want to create the transit VNet.

The locations available are based on the commercial cloud or GovCloud selection.

Step 6 Add a transit VNet:

a) In the **Transit VNet Name** field, type a name for the transit VNet.

   The name can contain 32 alphanumeric characters, hyphens (–), and underscore (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VNet:

   1. In the **WAN Edge Version** drop-down list, choose the software version to run on the transit VNet. The drop-down list includes the published versions of the device software in the Microsoft Azure marketplace.
   2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of theCisco Catalyst SD-WAN cloud devices that run on the transit VNet.
      - See Supported Instance Types for Cisco CSR1000V in the *Cisco CSR 1000v Deployment Guide for Microsoft Azure*.
      - See Supported Instance Types for Cisco Catalyst 8000V in the *Deploying Cisco Catalyst 8000V on Microsoft Azure*.

      Note
      We recommend that you choose the following size:

      For Cisco CSR1000V and Cisco Catalyst 8000V, choose DS3 instance type with four or more than four vCPUs such as, Standard DS3 v2 (4vCPU).

   3. To set up the transit VNet devices for Direct Internet Access (DIA), click one of the following:
      - **Disabled**: No Internet access.
      - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.

- **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.

4. In the **Device 1** drop-down list, choose the serial number of the first device.
5. In the **Device 2** drop-down list, choose the serial number of the second device in the device pair.
6. Click **Advanced** if you wish to enter more specific configuration options.
7. In the **Transit VNet CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you leave this field empty, the Transit VNet is created with a default CIDR of 10.0.0.0/16.

c) To complete the transit VNet configuration. click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

Step 7 Map host VNets to transit VNets:

a) In the **Select an account to discover** drop-down list, choose your Azure subscription ID.
Alternatively, to add a new Azure account from which you wish to discover host VNets, click **New Account**.

b) Click **Discover Host VNets**.

c) In the **Select a VNet** drop-down list, choose a desired host VNet.

d) Click **Next**.

e) From the table of host VNets, choose a desired host VNet.

f) Click **Map VNets**. The Map Host VNets pop-up appears.

g) In the **Transit VNet** drop-down list, choose the transit VNet to map to the host VNets.

h) In the **VPN** drop-down list, choose a VPN in the overlay network in which to place the mapping.

i) In the IPSec Tunnel CIDR section, to configure IPSec tunnels to reach the Azure virtual network transit, enter two pairs of interface IP addresses and a pair of loopback IP addresses for each of the Cisco CSR1000V or Cisco Catalyst 8000V devices . Ensure that the IP addresses are network addresses in the /30 subnet, unique across the overlay network, and they aren't part of the host VNet CIDR. If they are part of the host VNet CIDR, Microsoft Azure returns an error when attempting to create VPN connections to the transit VNet.

Note
The IP addresses aren't part of the host VNet and Transit VPC CIDR.

Microsoft Azure supports single Virtual Private Gateway (VGW) configuration over IPSec tunnels with redundancy provided over a single tunnel. Therefore, Cisco Catalyst SD-WAN Cloud OnRamp for IaaS supports two VGWs for redundancy. During a planned maintenance or an unplanned event of a VGW, the IPSec tunnel from the VGW to the cloud devices get disconnected. This loss of connectivity causes the cloud devices lose BGP peering with Cisco SD-WAN Manager over IPSec tunnel. To enable BGP peering with the cloud routers rather than the IP address of the IPSec tunnel, provide the loopback addresses for each cloud device.

Note
The loopback option for BGP peering supports single and multiple Virtual Gateways, or Customer Gateway configuration or both on Azure cloud. The loopback option applies only to the new host VNets mapped to transit VNets and not on the existing VNets.

j) In the Azure Information section:

1. In the **BGP ASN** field, enter the ASN that you configure on the Azure Virtual Network Gateway, which is brought up within the host VNet. Use an ASN that isn't part of an existing configuration on Azure. For acceptable ASN values, refer to Microsoft Azure documentation.

2. In the **Host VNet Gateway Subnet** field, enter a host VNet subnet in which the Virtual Network Gateway can reside. We recommend you use a /28 subnet or higher. Ensure not to provide a subnet that is already created in the VNet.

   Note
   Ensure that there's an unused CIDR inside the host VNet CIDR.

k) Click **Map VNets**.
l) Click **Save and Complete**.

Note
When configuring the VPN feature template for VPN 0 for the two Cisco Catalyst SD-WAN cloud devices that form the transit VNet, ensure that the color you assign to the tunnel interface is a public color, and not a private color. Public colors are:

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

The **Task View** screen appears, confirming that the host VNet has been mapped to the transit VNet successfully.

The creation of VNet Gateway can take up to 45 minutes.

Manage Host and Transit VNets

Display Host VNets

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

By default, the **Mapped Host VNets** field is selected and the table under mapped host VNets list the mapped host and transit VNets, the state of the transit VNets, and the VPN ID.

Step 2 To list unmapped host VNets, click **Un-Mapped Host VNets**. Then click **Discover Host VNets**.

Step 3 To display the transit VNets, click **Transit VNets**.

Map Host VNets to an Existing Transit VNet

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

Step 2 Click **Un-Mapped Host VNets**.

Step 3 Click **Discover Host VNets**.

Step 4 From the list of discovered host VNets, choose the desired host VNets.

Step 5 Click **Map VNet**. The Map Host VNets pop-up opens.

Step 6 From the **Transit VNet** drop-down list, choose the desired transit VNet.

Step 7 From the **VPN** drop-down list, choose the VPN in the overlay network in which to place the mapping.

Step 8 Click **Map VNets**.

Unmap Host VNets

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

Step 2 Click **Mapped Host VNets**.

Step 3 From the list of VNets, choose the desired host VNets. We recommend that you unmap one VNet at a time. If you want to unmap multiple VNets, don't choose more than three in a single unmapping operation.

Step 4 Click **Un-Map VNets**.

Step 5 Click **OK** to confirm the unmapping.

Display Transit VNets

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

Step 2 Click **Transit VNets**.

A table lists all the transit VNets.

Add Transit VNet

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

Step 2 Click **Transit VNets**.

Step 3 Click **Add Transit VNet**.

To add a transit VNet, follow the instructions in step 5 of Configure Cisco Catalyst SD-WAN Cloud OnRamp for IaaS on Microsoft Azure, on page 25.

Delete Transit VNet

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Click the desired VNet. The **Host VNets/Transit VNets** window opens.

Step 2 Click **Mapped Host VNets**.

Step 3 Choose the desired host VNet, and click **Un-Map VNets**.

Ensure that you unmap all host VNets that are mapped to the transit VNet that you want to delete.

Step 4 Click **OK** to confirm the unmapping.

Step 5 Click **Transit VNets**.

Step 6 For the desired transit VNet to be deleted, click the trash icon.

Step 7 Click **OK** to confirm.

Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

This section describes how to troubleshoot common problems with Cisco Catalyst SD-WAN Cloud OnRamp for IaaS.

Two Cisco CSR1000V or Cisco Catalyst 8000V Devices are Not Available

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. After you click **Add New Cloud Instance**, you see an error message indicating that two Cisco CSR1000V or Cisco Catalyst 8000V devices aren't available.

Resolve the Problem

The Cisco SD-WAN Manager server doesn't have two Cisco CSR1000V or Cisco Catalyst 8000V devices that are running licensed Cisco Catalyst SD-WAN software. Contact your operations team so that they can create the necessary Cisco CSR1000V or Cisco Catalyst 8000V devices.

If the Cisco CSR1000V or Cisco Catalyst 8000V devices are present and the error message persists, then the two devices aren't attached to configuration templates. Attach these templates in the Cisco SD-WAN Manager **Configuration** > **Templates** Device window. For the desired device templates, click **…** and choose **Attach Devices**.

Required API Permissions are Unavailable

When you enter your API keys, you get an error message indicating that this user doesn't have the required permissions.

Resolve the Problem

Ensure that the Cisco SD-WAN Manager server can reach the internet and has a DNS server configured so that it can reach AWS or Microsoft Azure. To configure a DNS server, in the Cisco SD-WAN Manager VPN feature configuration template, enter the IP address of a DNS server, and then reattach the configuration template to the Cisco SD-WAN Manager server.

For AWS, check the API keys belonging to your AWS account. If you think you have the wrong keys, generate another pair of keys.

For AWS, if you're entering the correct keys and the error message persists, the keys don't have the required permissions. Check the user permissions associated with the key. Give necessary permissions to the user to create and edit VPCs and EC2 instances.

If the error message persists, check the time of the Cisco SD-WAN Manager server to ensure that it's set to the current time. If it's not, configure the Cisco SD-WAN Manager server time to point to the Google NTP server. To configure the server time, in the Cisco SD-WAN Manager NTP feature configuration template, enter the hostname of an NTP server. Next, reattach the configuration template to the NTP feature using Cisco SD-WAN Manager. The Google NTP servers are time.google.com, time2.google.com,time3.google.com, and time4.google.com, and so on.

WAN Edge Router Software Versions don't Appear in the Drop-Down When Configuring for AWS

Problem Statement

When you're trying to configure transit VPC parameters for the transit VPC, Cisco CSR1000V and Cisco Catalyst 8000V devices software versions aren't listed in the drop-down list.

Resolve the Problem

Ensure that you subscribe to the Cisco CSR1000V or Cisco Catalyst 8000V devices Amazon machine image (AMI) in your account within the AWS Marketplace.

Ensure that the Cisco CSR1000V is using software Release 16.12.1b or later and Cisco Catalyst 8000V is using software Release 17.4.1a or later.

VPNs aren't Listed During Configuration

Problem Statement

After you select the host VPCs or VNets to map, VPNs aren't listed in the drop-down list.

Resolve the Problem

The problem occurs when the device configuration template attached to the Cisco Catalyst SD-WAN cloud devices doesn't include service-side VPNs. You require the service-side VPNs (VPNs other than VPN 0 and VPN 512) to configure the IPsec connection between the two Cisco Catalyst SD-WAN cloud devices that you select for the transit and host VPCs or VNets.

This problem can also occur if the two Cisco Catalyst SD-WAN cloud devices that you select for the transit VPC or VNet have no overlapping service-side VPNs. Because the two Cisco Cloud Services router 1000V or Cisco Catalyst 8000V devices form an active–active pair, configure the same service-side VPNs on both of them.

To configure service-side VPNs, in the Cisco SD-WAN Manager VPN feature configuration template, configure at least one service-side VPN. Ensure that at least one of the service-side VPNs is the same on both routers. Then reattach the configuration template to the routers.

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS Task Fails

Problem Statement

After you have completed mapping the host VPCs to the transit VPCs, or host VNets to transit VNets, the configuration of Cisco Catalyst SD-WAN Cloud OnRamp for IaaS fails.

Resolve the Problem

Review the displayed task information that appears on the screen to determine why the task failed. If the errors are related to AWS or Azure resources, ensure that all required resources are in place.

Cisco Catalyst SD-WAN Cloud OnRamp for IaaS Task Succeeds, but Cisco Catalyst SD-WAN Cloud Devices Are Down

Problem Statement

The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS task was successful, but the Cisco Catalyst SD-WAN cloud devices are still in the down state.

Resolve the Problem

Check the configuration templates:

- Check that all portions of the Cisco Catalyst SD-WAN cloud devices configuration, including policies, are valid and correct. If the configurations are invalid, they aren't applied to the router, and the router never comes up.
- Check that the configuration for the Cisco Catalyst SD-WAN Validator is correct. If the DNS name or IP address configured in the Cisco Catalyst SD-WAN Validator is wrong, the Cisco CSR1000V or Cisco Catalyst 8000V device are unable to reach the Cisco Catalyst SD-WAN Validator, and hence they are unable to join the overlay network.

After you have determined what the configuration issues are:

1. Delete the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS components:
   a. Unmap the host VPCs or VNets and the transit VPCs or VNets.
   b. Delete the transit VPC for Cisco CSR1000V or Cisco Catalyst 8000V devices.
2. Edit the configuration templates and reattach them to the Cisco Catalyst SD-WAN cloud devices.
3. Repeat the Cisco Catalyst SD-WAN Cloud OnRamp for IaaS configuration process.

Desired Routes are Not Exchanged

Problem Statement

The Cisco Catalyst SD-WAN Cloud OnRamp for IaaS configuration workflow is successful, the Cisco CSR1000V or Cisco Catalyst 8000V devices are available and running, but the desired routes aren't getting exchanged.

Resolve the Problem

In Cisco SD-WAN Manager, check the BGP configuration on the transit cloud routers. During the mapping process, when you configureCisco Catalyst SD-WAN Cloud OnRamp for IaaS service, BGP is configured to advertise the network address, 0.0.0.0/0. Make sure that the service-side VPN contains an IP route that points to 0.0.0.0/0. If necessary, add a static route in the VPN feature configuration template, and then reattach the configuration to the two cloud routers that you selected for the transit VPC or VNet.

On AWS, go to the host VPC and check the route table. In the route table, click **Enable route propagation** to ensure that the VPC receives the routes.

End-to-End Ping Is Unsuccessful

Problem Statement

Routing is working properly, but an end-to-end ping isn't working.

Resolve the Problem

On AWS, check the security group rules of the host VPC. On Azure, check the network security group rules of the host VNet. The security group rules must allow the source IP address range subnets of the on-premises or branch-side devices to allow traffic from the branch to reach AWS.

Sample Feature Template Settings

Feature Templates

The following is a sample of the various feature templates settings for Cisco CSR1000V, Cisco Catalyst 8000V devices.

System Feature Template

Template: Basic Information/Cisco System

Template Name: Cisco_System_cEdge_Template

Description: System Template

Table 2: System feature template settings

Section	Parameter	Type	Variable/Value
Basic Configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_host_name
	Device Groups	Device Specific	system_device_groups
	Console Baud Rate	Global	115200
GPS	Latitude	Device Specific	system_latitude
	Longitude	Device Specific	system_longitude
Advanced	Port Hopping	Device Specific	system_port_hop
	Port Offset	Device Specific	system_port_offset

Logging Feature Template

Template: Other Templates/Cisco Logging

Template Name: Cisco_Logging_cEdge_Template

Description: Logging Template

Table 3: Logging feature template settings

Section	Parameter	Type	Variable/Value
Server (Optional)	Hostname/IP address	Global	10.1.0.68
	VPN ID	Device Specific	logging_server_vpn

The logging server is optional within the Logging_Template.

BFD Feature Template

Template: Basic Information/Cisco BFD_Template

Template Name: BFD_cEdge_Template

Description: BFD Template

Table 4: BFD feature template settings

Section	Parameter	Type	Variable/Value
Basic Configuration	Poll Interval	Global	120000
Color (Biz Internet)	Color	Drop-down list	Biz Internet
	Hello Interval (milliseconds)	Device Specific	biz_internet_bfd_hello_interval
	Path MTU	Global	Off

VPN512 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN512_Template_cEdge_Template

Description: VPN 512 Out-of-Band Management

Table 5: VPN512 feature template settings

Section	Parameter	Type	Variable/Value
Basic Configuration	VPN	Global	512
	Name	Global	Management VPN

VPN512 Interface Ethernet Feature Template

Template: VPN / Cisco VPN Interface Ethernet

Template Name: Cisco_Transit_VPN512_Interface_Template_cEdge_Template

Description: VPN 512 Management Interface

Table 6: VPN512 Interface Ethernet feature template settings

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgmt_int
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio Button	Dynamic

NTP Feature Template

Template: Basic Information/Cisco NTP

Template Name: Cisco_NTP_cEdge_Template

Description: NTP Template

Table 7: NTP feature template settings

Section	Parameter	Type	Variable/Value
Server	Hostname/IP address	Global	time.nist.gov

You should be careful to use only known and trusted NTP servers. Disruptions to time synchronizations can affect the ability of the Cisco Catalyst SD-WAN Cloud devices within the transit VPC or transit VNet to connect to the Cisco SD-WAN Control Components, and the ability to establish IPsec connections to other Cisco Catalyst SD-WAN devices.

AAA Feature Template

Template: Basic Information/Cisco AAA

Template Name: Cisco_AAA_cEdge_Template

Description: AAA Template

Table 8: Cisco AAA feature template settings

Section	Parameter	Type	Variable/Value
Local	User/admin/Password	Global	<your admin password>
	User/admin/Privilege	Global	15
AAA	ServerGroups priority order	Global	local

OMP Feature Template

Template: Basic Information/Cisco OMP

Template Name: Cisco_OMP_cEdge_Template

Description: OMP Template

Table 9: Cisco OMP feature template settings

Section	Parameter	Type	Variable/Value
OMP	Number of Paths Advertised per Prefix	Global	Factory_Default_Cisco_OMP__ipv46_Template

Security Feature Template

Template: Basic Information/Cisco Security

Template Name: Cisco_Security_cEdge_Template

Description: Security Template

Table 10: Security feature template settings

Section	Parameter	Type	Variable/Value
Security	Replay window	Global/drop-down list	Factory_Default_Cisco_Security_Template

VPN0 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN0_cEdge_Template

Description: VPN0 Transport Template

Table 11: VPN0 feature template settings

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN

VPN0 Interface Feature Template

Template: VPN/Cisco VPN Interface Ethernet

Template Name: Cisco_Transit_VPN0_cEdge_gigabit-ethernet2

Description: VPN0 Transport Interface

Table 12: Cisco VPN0 interface feature template settings

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Drop-down list	GigabitEthernet2/
	Description	Global	Internet Interface
IPv4 Configuration	IPv4 Address	Radio Button	Dynamic
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
	Allow Service>All	Global	On
Tunnel > **Advanced Options** > **Encapsulation**	IPsec Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350

VPN1 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN1_cEdge_Template

Description: VPN1 Service Template

Table 13: VPN1 feature template settings

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN 1
	Enhance ECMP Keying	Global	On
Advertise OMP	BGP (IPv4)	Global	On
	Connected (IPv4)	Global	On

VPN2 Feature Template

Template: VPN/Cisco VPN

Template Name: Cisco_Transit_VPN2_cEdge_Template

Description: VPN2 Service Template

Table 14: VPN2 feature template settings

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	2
	Name	Global	Service VPN 2
	Enhance ECMP Keying	Global	On
Advertise OMP	BGP (IPv4)	Global	On

Device Templates

The following table summarizes the device template for the Cisco CSR1000V or Cisco Catalyst 8000V devices.

Template Name: Cloud_OnRamp_cEdge_Template

Table 15: Transit VPC or Transit VNet Device Template

Template Type	Template Sub-Type	Template Name
Cisco System		Cisco_System_cEdge_Template
	Cisco Logging	Cisco_Logging_cEdge_Template
	Cisco NTP	Cisco_NTP_cEdge_Template
	Cisco AAA	Cisco_AAA_cEdge_Templatee
Cisco BFD		BFD_cEdge_Template
Cisco OMP		Cisco_OMP_cEdge_Template
Cisco Security		Cisco_Security_cEdge_Template
Cisco VPN0		Cisco_Transit_VPN0_cEdge_Template
	Cisco VPN Interface Ethernet	Cisco_Transit_VPN0_cEdge_gigabit-ethernet2
Cisco VPN512		Cisco_Transit_VPN512_Template_cEdge_Template
	Cisco VPN Interface Ethernet	Cisco_Transit_VPN512_Interface_Template_cEdge_Template
Cisco VPN1		Cisco_Transit_VPN1_cEdge_Template

Template Type	Template Sub-Type	Template Name
VPN2		Cisco_Transit_VPN2_cEdge_Template

Sample Device Template Variable Values

The following sample information provides the device template variable values that you can use for the first and second Cisco CSR1000V or Cisco Catalyst 8000V devices.

Table 16: Cisco CSR1000V or Cisco Catalyst 8000V Device Template Variable Values for First Device

Variable	Value
Hostname(system_host_name)	CSR_CoR1
System IP(system_system_ip)	209.165.200.225
Site ID(system_site_id)	115001

Table 17: Cisco CSR1000V or Cisco Catalyst 8000V Device Template Variable Values for Second Device

Variable	Value
Hostname(system_host_name)	CSR_CoR2
System IP(system_system_ip)	209.165.201.1
Site ID(system_site_id)	115001

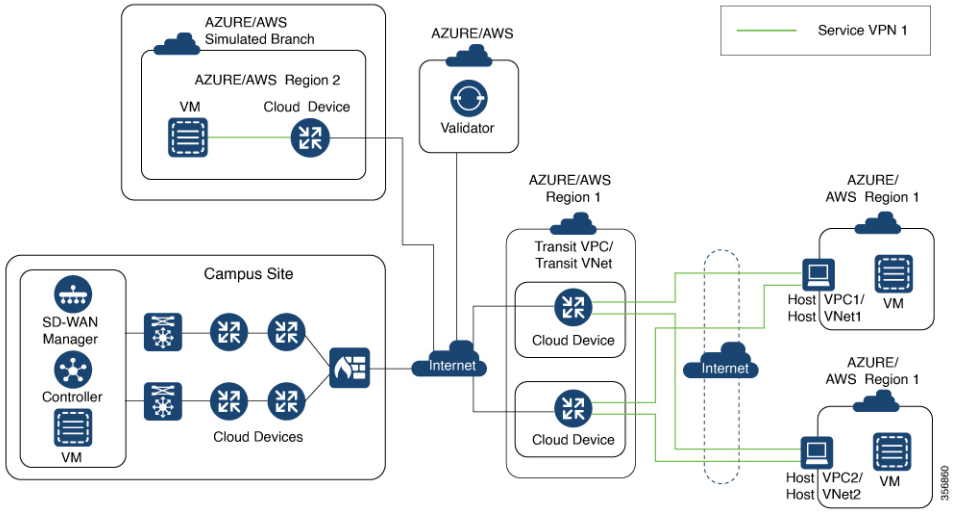
Example for Cisco Catalyst SD-WAN Cloud OnRamp for IaaS

In this example, a single transit VPC or VNet is created within an AWS or Microsoft Azure region and you map two existing host VPCs or VNets within the same region to a transit VPC or VNet. Then, you can access the host VPCs or VNets from a campus and a simulated branch location.

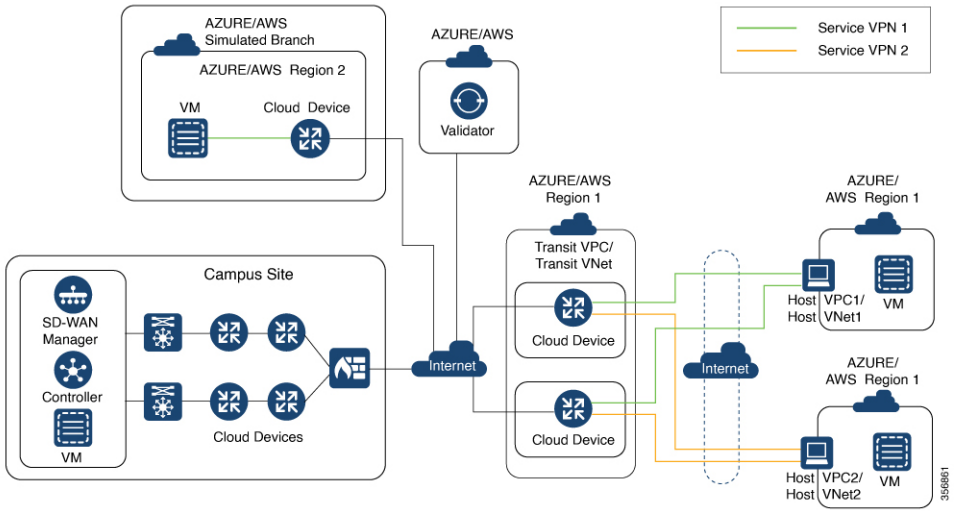
Cisco Catalyst SD-WAN deployments implement connectivity using different VPNs that range 0–512. VPN 0 represents the transport (WAN) network and VPN 512 represents the management network. Use the remaining VPNs (1–511) as service VPNs. The following two scenarios to deploy Cisco Catalyst SD-WAN Cloud OnRamp for IaaS are considered:

- Full connectivity: Map both host VPCs or VNets to service VPN 1 within the transit VPC or VNet. You can configure service VPN 1 on the service-side of Cisco CSR1000V or Cisco Catalyst 8000V devices deployed within the campus, and Cisco CSR1000V or Cisco Catalyst 8000V devices deployed within the simulated branch. This connectivity allows communication from both the campus and the branch sites to AWS Elastic Compute Cloud (EC2) instances within either of the host VPCs. The connectivity also allows communication between AWS or Azure EC2 instances deployed within the two host VPCs. The deployment demonstrates a scenario where all entities within the organization have full connectivity

to the public cloud resources deployed by the organization. The following image illustrates the first scenario.



- Segmentation to the cloud provider: Map one of the host VPCs or VNets to service VPN 1 and the other host VPC or VNet to service VPN 2 within the transit VPC or VNet. This mapping provides segmentation and therefore traffic isolation between the two host VPCs or VNets. You can configure the campus only for service VPN 1, and allowing it to communicate with AWS or Azure EC2 instances within the first host VPC. Configure the branch for service VPN 2, allowing it to communicate with AWS or Azure EC2 instances within the second host VPC. This deployment demonstrates a scenario where different entities within an organization require access only to specific public cloud resources. The following figure illustrates the second scenario.



Map Host VPCs or VNets to the Transit VPC or VNet in the Same Service VPN

To map both host VPCs or VNets to service VPN 1 within the transit VPC or VNet, perform the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Choose both the host VPCs or host VNets that you want to map, and click **Map VPCs** or **Map VNets**.

The **Map Host VPCs** or **Map Host VNets** pop-up opens.

2. In the **Transit VPC** or **Transit VNet** drop-down list, choose the transit VPC or VNet to map to the host VPCs or VNets.
3. In the **VPN** drop-down list, select **1**.

   Mapping host VPCs or host VNets to the same service VPN allows communication between the host VPCs or VNets.
4. For AWS configuration, disable **Route Propagation**.

   Enabling route propagation propagates the BGP routes to the host VPC selected for mapping.
5. Click **Map VPCs** or **Map VNets**.

   After a few minutes, the Task View window appears, confirming that the host VPC or VNet has been mapped to the transit VPC or VNet.

These steps complete the mapping of both the host VPCs or VNets to service VPN 1. You can verify connectivity between EC2 instances with each host VPC or VNet by establishing an SSH connection between them. Similarly, by mapping both the campus and branch to service VPN 1, you can verify connectivity to both host VPCs or VNets by establishing SSH connections from the campus and branch to the EC2 instances within the host VPCs or VNets.

Map Each Host VPC or VNet to the Transit VPC or VNet in Different Service VPNs

To map one host VPC or VNet to service VPN 1; while the other host VPC or VNet to service VPN 2, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for IaaS**. Choose the host VPC or VNet that you want to map, and click **Map VPCs** or **Map VNets**.

   The **Map Host VPCs** or **Map Host VNets** pop-up opens.
2. In the **Transit VPC** or **Transit VNet** drop-down list, choose the transit VPC or VNet to map to the host VPCs or VNets.
3. In the **VPN** drop-down list, choose **1**.

   The first host VPC or VNet is now mapped to service VPN 1.
4. Click **Map VPCs** or **Map VNets**.

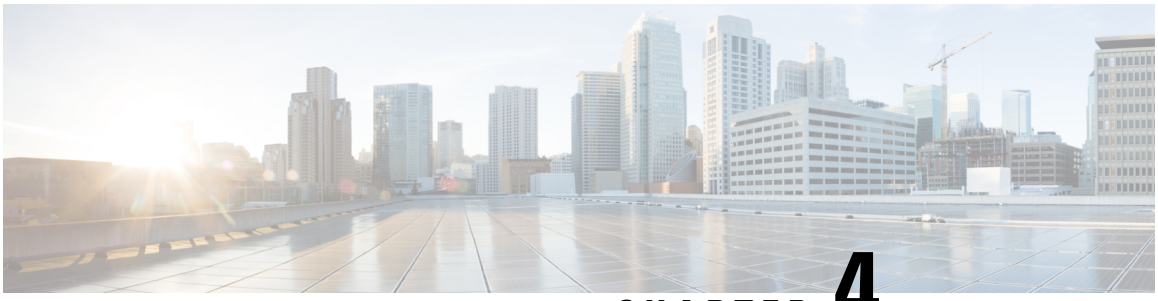
   After a few minutes, the Task View window appears, confirming that the host VPC or VNet has been mapped to the transit VPC or VNet.
5. Repeat Steps 1–3 for the second host VPC or VNet

   When selecting the VPN value, map the host VPC or VNet to service VPN 2.

This process completes the mapping of the first host VPC or VNet to service VPN 1 and the second host VPC or VNet to service VPN 2.

By mapping the campus to service VPN 1, you can verify connectivity to the first host VPC or VNet by establishing SSH connections from the campus to the EC2 instances within that host VPC or VNet. However, SSH connections from the campus to the EC2 instances within the second host VPC or VNet can’t be established. By mapping the branch to service VPN 2, you can verify connectivity to the second host VPC or VNet by establishing SSH connections from the branch to the EC2 instances within that host VPC or VNet.

However, SSH connections from the branch to the EC2 instances within the first host VPC or VNet can’t be established.



CHAPTER 4

Cloud OnRamp for Colocation

As more applications move to the cloud, the traditional approach of backhauling traffic over expensive WAN circuits to a data center is no longer relevant. The conventional WAN infrastructure was not designed for accessing applications in the cloud. The infrastructure is expensive and introduces unnecessary latency that degrades the experience.

Network architects are reevaluating the design of the WANs to achieve the following:

- Support a cloud transition.
- Reduce network costs.
- Increase the visibility and manageability of the cloud traffic.

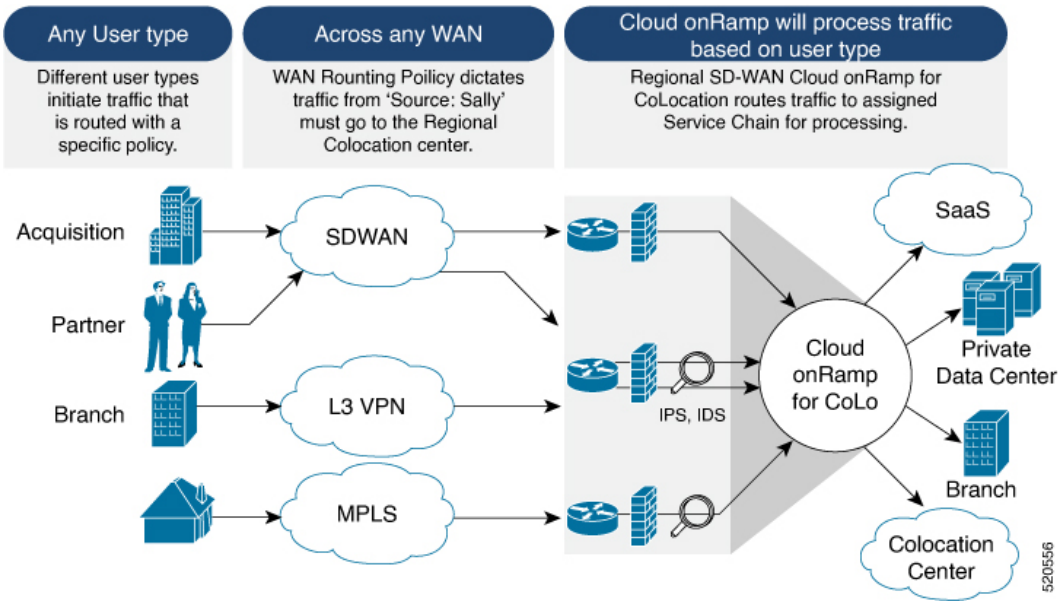
The architects are turning to Software-Defined WAN (SD-WAN) fabric to take advantage of inexpensive broadband Internet services and to route intelligently a trusted SaaS cloud-bound traffic directly from remote branches.

With the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution built specifically for colocation facilities, the solution routes the traffic to the best-permissible path from branches and remote workers to where all applications are hosted. The solution also allows distributed enterprises to have an alternative to enabling direct internet access at the branch and enhance their connectivity to infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) providers.

The solution provides enterprises with multiple distributed branch offices that are clustered around major cities or spread over several countries the ability to regionalize the routing services in colocation facilities. Reason being, these facilities are physically closer to the branches and can host the cloud resources that the enterprise needs to access. So, essentially by distributing a virtual Cisco Catalyst SD-WAN over a regional architecture of colocation centers, the processing power is brought to the cloud edge.

The following image shows how you can aggregate the access to the multicloud applications from multiple branches to regional colocation facilities.

Figure 2: Cisco Catalyst SD-WAN Cloud OnRamp for Colocation



The solution can serve four specific types of enterprises:

- Multinational companies that cannot use direct internet connections to the cloud and SaaS platforms due to security restrictions and privacy regulations.
- Partners and vendors without Cisco Catalyst SD-WAN but still need connectivity to their customers. They do not want to install Cisco Catalyst SD-WAN routing appliances in their site.
- Global organizations with geographically distributed branch offices that require high bandwidth, optimum application performance, and granular security.
- Remote access that need secure VPN connections to an enterprise over inexpensive direct internet links.

The Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution can be hosted within certain colocation facilities by a colocation IaaS provider. You can select the colocation provider that meets your needs in a region on a regional basis as long as it supports the necessary components.

- Deploy Cloud OnRamp for Colocation Solution, on page 46
- Manage Cloud OnRamp for Colocation Devices, on page 48
- Manage Clusters , on page 50
- Manage Service Groups, on page 75
- Manage VM Catalog and Repository, on page 92
- Monitor Operational Status of Cloud OnRamp for Colocation Devices from Cisco Catalyst SD-WAN Manager, on page 104
- Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Multitenancy, on page 114

Deploy Cloud OnRamp for Colocation Solution

This topic outlines the sequence of how to get started with the colo devices and build clusters on Cisco SD-WAN Manager. Once a cluster is created and configured, you can follow the steps that are required to

activate the cluster. Understand how to design service groups or service chains and attach them to an activated cluster. The supported Day-N operations are also listed in this topic.

1. Complete the solution prerequisites and requirements. See Prerequisites and Requirements of Cloud OnRamp for Colocation Solution .
   - Complete wiring the CSP devices (set up CIMC for initial CSP access) and Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches (set up console server) along with OOB or management switches. Power on all devices.
   - Set up and configure DHCP server. See Provision DHCP Server per Colocation.
2. Verify the installed version of Cisco NFVIS and install NFVIS, if necessary. See Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP.
3. Set up or provision a cluster. A cluster constitutes of all the physical devices including CSP devices, and Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. See Get Started with Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution.
   - Bring up CSP devices. See Bring Up Cloud Services Platform Devices.
   - Bring up Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. See Bring Up Switch Devices.
   - Provision and configure a cluster. See Provision and Configure Cluster.

     Configure a cluster through cluster settings. See Cluster Settings.
4. Activate a cluster. See Create and Activate Clusters, on page 52.
5. Design service group or service chain. See Manage Service Groups, on page 75.

Note You can design a service chain and create a service group anytime before creating clusters or activating clusters after all VMs are uploaded to the repository.

6. Attach or Detach service group and service chains to a cluster. See Attach or Detach a Service Group in a Cluster, on page 91.

Note Service chains can be attached to a cluster after the cluster is active.

7. (Optional) Perform all Day-N operations.
   - Detach a service group to detach service chains. See Attach or Detach a Service Group in a Cluster, on page 91.
   - Add and delete CSP devices from a cluster. See Add Cloud OnRamp Colocation Devices , on page 48 and Delete Cloud OnRamp for Colocation Devices , on page 49.
   - Deactivate a cluster. See Remove Cluster , on page 74.
   - Reactivate a cluster. See Reactivate Cluster , on page 74.

- Design more service group or service chain. See Create Service Chain in a Service Group, on page 75.

Manage Cloud OnRamp for Colocation Devices

You can add CSP devices, Catalyst 9500-40X devices, and VNFs through Cisco SD-WAN Manager.

Add Cloud OnRamp Colocation Devices

You can add CSP devices, switch devices, and VNFs using Cisco SD-WAN Manager. When you order the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution product identifier (PID), the device information is available from the smart account that can be accessed by Cisco SD-WAN Manager.

Before you begin

Ensure that the setup details are as follows:

- Cisco Catalyst SD-WAN setup details such as, Cisco SD-WAN Manager IP address and credentials, Cisco SD-WAN Validator IP address and credentials
- NFVIS setup details such as, Cisco CSP device CIMC IP address and credentials or UCSC CIMC IP address and credentials
- Able to access both the switch consoles

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal** to start an SSH session with Cisco SD-WAN Manager.

Step 2 Choose a CSP device or a switch device.

Step 3 Enter the username and password for the CSP device or switch device, and click **Enter**.

Step 4 Get the PID and serial number (SN) of a CSP device.

The following sample output shows the PID for one of the CSP devices.

```
CSP# show pl
platform-detail hardware_info Manufacturer "Cisco Systems Inc"
platform-detail hardware_info PID CSP-5444
platform-detail hardware_info SN WZP224208MB
platform-detail hardware_info hardware-version 74-105773-01
platform-detail hardware_info UUID da39edec-d831-e549-b663-9e407afd5ac6
platform-detail hardware_info Version 4.6.0-15
```

The output shows both the CSP device PID and serial number.

Step 5 Get the serial number of both the Catalyst 9500 switch devices.

The following sample shows the serial number of the first switch.

```
Switch1# show version
Cisco IOS XE Software, Version 17.03.03
```

```
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Fri 26-Feb-21 02:01 by mcpre
Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                  Technology-package
Current                       Type                     Next reboot
------------------------------------------------------------------------------
network-advantage    Smart License                  network-advantage
dna-advantage        Subscription Smart License     dna-advantage
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C9500-40X (X86) processor with 1331521K/6147K bytes of memory.
Processor board ID FCW2229A0RK
1 Virtual Ethernet interface
96 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-1:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-1:.

Base Ethernet MAC Address          : 00:aa:6e:f3:02:00
Motherboard Assembly Number        : 73-18140-03
Motherboard Serial Number          : FOC22270RF8
Model Revision Number              : D0
Motherboard Revision Number        : B0
Model Number                       : C9500-40X
System Serial Number               : FCW2229A0RK
CLEI Code Number                   :
```

From this output, you can know the Catalyst 9500 switch series and the serial number.

Step 6 Create a .CSV file with the PID and serial number records for all the CSP devices and Catalyst 9500 switches in a colocation cluster.

For example, from the information available from Steps 4,5, the CSV-formatted file can be as follows:

```
C9500-40,FCW2229A0RK CSP-5444,SN WZP224208MB
```

Note
You can create a single .CSV file for all devices in a colocation cluster.

Step 7 Upload all the CSP and switch devices using Cisco SD-WAN Manager. For more information, see Uploading a device authorized serial number file.

After upload, you can see all the CSP and switch devices listed in the table of devices.

Delete Cloud OnRamp for Colocation Devices

To delete the CSP devices from Cisco SD-WAN Manager, perform the following steps:

Before you begin

Ensure that you consider the following:

- If any service chains are attached to a device that is deleted, detach service groups. See Attach or Detach a Service Group in a Cluster, on page 91.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

Step 2 For the desired device, click **…** and choose **Invalid**.

Step 3 In the **Configuration** > **Certificates** window, click **Send to Controller**.

Step 4 In the **Configuration** > **Devices** window, for the desired device, click **…** and choose **Delete WAN Edge**.

Step 5 Click **OK** to confirm the deletion of the device.

Deleting a device removes the serial and chassis numbers from the **WAN edge router serial number** list, and also permanently removes the configuration from Cisco SD-WAN Manager.

Manage Clusters

Use the Cloud OnRamp for Colocation screen to configure a colocation cluster and service groups that can be used with the cluster.

The three steps to configure are:

- Create a cluster.
- Create a service group.
- Attach a cluster with a service group.

A colocation cluster is a collection of two to eight CSP devices and two switches. The supported cluster templates are:

- Small cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+2 CSP
- Medium Cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+4 CSP
- Large Cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+6 CSP
- X-Large Cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+8 CSP



Note Ensure that you add a minimum of two CSP devices one-by-one to a cluster. You can keep adding three, four, and so on, up to a maximum of eight CSP devices. You can edit a Day-N configuration of any cluster, and add pairs of CSP devices to each site up to a maximum of eight CSP devices.

Ensure that all devices that you bring into a cluster have the same software version.

Note You can't use the CSP-5444 and CSP-5456 devices in the same cluster.

Following are the cluster states:

- Incomplete—When a cluster is created from the Cisco SD-WAN Manager interface without providing the minimum requirement of two CSP devices and two switches. Also, cluster activation is not yet triggered.
- Inactive—When a cluster is created from the Cisco SD-WAN Manager interface after providing the minimum requirement of two CSP devices and two Switches, and cluster activation is not yet triggered.
- Init—When the cluster activation is triggered from the Cisco SD-WAN Manager interface and Day-0 configuration push to the end devices is pending.
- Inprogress—When one of the CSP devices within a cluster comes up with control connections, the cluster moves to this state.
- Pending—When the Day-0 configuration push is pending or VNF install is pending.
- Active—When a cluster is activated successfully and NCS has pushed the configuration to the end device.
- Failure—If Cisco Colo Manager has not been brought up or if any of the CSP devices that failed to receive an UP event.

A cluster transitioning to an active state or failure state is as follows:

- **Inactive** > **Init** > **Inprogress** > **Pending** > **Active**—Success
- **Inactive** > **Init** > **Inprogress** > **Pending** > **Failure**—Failure

Provision and Configure Cluster

This topic describes about activating a cluster that enables deployment of service chains.

To provision and configure a cluster, perform the following:

1. Create a colocation cluster by adding two to eight CSP devices and two switches.

   CSP devices can be added to a cluster and configured using Cisco SD-WAN Manager before bringing them up. You can configure CSP devices and Catalyst 9K switches with the global features such as, AAA, default user (admin) password, NTP, syslog, and more.

2. Configure colocation cluster parameters including IP address pool input such as, service chain VLAN pool, VNF management IP address pool, management gateway, VNF data plane IP pool, and system IP address pool.

3. Configure a service group.

   A service group consists of one or more service chains.

Note You can add a service chain by selecting one of the predefined or validated service chain template, or create a custom one. For each service chain, configure input and output VLAN handoff and service chain throughput or bandwidth, as mentioned.

4. Configure each service chain by selecting each VNF from the service template. Choose a VNF image that is already uploaded to the VNF repository to bring up the VM along with required resources (CPU, memory, and disk). Provide the following information for each VNF in a service chain:
   - The specific VM instance behavior such as, HA, shared VM can be shared across service chains.
   - Day-0 configuration values for tokenized keys and not part of the VLAN pool, management IP address, or data HA IP address. The first and last VMs handoff-related information such as peering IP and autonomous system values must be provided. The internal parameters of a service chain are automatically updated by Cisco SD-WAN Validator from the VLAN, or Management, or Data Plane IP address pool provided.
5. Add the required number of service chains for each service group and create the required number of service groups for a cluster.
6. To attach a cluster to a site or location, activate the cluster after all configuration is complete.

   You can watch the cluster status change from In progress to active or error in the **Task View** window.

To edit a cluster:

1. Modify the activated cluster by adding or deleting service groups or service chains.
2. Modify the global features configuration such as, AAA, system setting, and more.

You can predesign a service group and service chain before creating a cluster. You can then attach the service group with a cluster after the cluster is active.

Create and Activate Clusters

This topic provides the steps on how you can form a cluster with CSP devices, Cisco Catalyst switches as a single unit, and provision the cluster with cluster-specific configuration.

Before you begin

- Ensure that you synchronize the clocks for Cisco SD-WAN Manager and CSP devices. To synchronize a clock for CSP devices, configure the NTP server for CSP devices when you enter information about cluster settings.
- Ensure that you configure the NTP server for Cisco SD-WAN Manager and Cisco SD-WAN Validator. To configure the NTP server.
- Ensure that you configure the OTP for the CSP devices to bring up the CSP devices.
- Ensure that you power on both the Catalyst 9500 switches and ensure that they are operational.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose Cisco SD-WAN Manager, click **Configuration** > **Cloud OnRamp for Colocation**.

a) Click **Configure & Provision Cluster**.

b) Provide the following information:

Table 18: Cluster Information

Field	Description
Cluster Name	The cluster name can contain 128 alphanumeric characters.
Description	The description can contain 2048 alphanumeric characters.
Site ID	The overlay network site identifier. Ensure that the value you enter for Site ID is similar to the organizations Site ID structure for the other Cisco Catalyst SD-WAN overlay elements.
Location	The location can contain 128 alphanumeric characters.
Cluster Type	To configure a cluster in a multitenant mode so that it can be shared across multiple tenants, choose **Shared**. **Note** In the single-tenant mode, the cluster type **Non Shared** is selected by default.

c) To configure switches, click a switch icon in the **Switches** box. In the **Edit Switch** dialog box, enter a switch name and choose the switch serial number from the drop-down list. Click **Save**.

The switch name can contain128 alphanumeric characters.

The switch serial numbers that you view in the drop-down list are obtained and integrated with Cisco SD-WAN Manager using the PnP process. These serial numbers are assigned to switches when you order Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution PID on the CCW and procure the switch devices.

Note
You can keep the serial number field blank for switch devices and CSP devices, design your colocation cluster, and then edit the cluster later to add the serial number after you procure the devices. However, you can't activate a cluster with the CSP devices or switch devices without the serial numbers.

d) To configure another switch, repeat Step c.

e) To configure CSP devices, click a CSP icon in the **Appliances** box. The **Edit CSP** dialog box is displayed. Provide a CSP device name and choose the CSP serial number from the drop-down list. Click **Save**.

The CSP device name can contain 128 alphanumeric characters.

f) Configure OTP for the CSP devices to bring up the devices.

g) To add remaining CSP devices, repeat Step e.

h) Click **Save**.
After you create a cluster, on the cluster configuration window, an ellipsis enclosed in a yellow circle appears next to a device where the serial number isn't assigned for the device. You can edit a device to enter the serial numbers.

i) To edit a CSP device configuration, click a CSP icon, and perform the process mentioned in substep e.

j) To set the mandatory and optional global parameters for a cluster, on the cluster configuration page, enter the parameters for **Cluster Configuration**.

k) Click **Save**.
You can view the cluster that you created in a table on the cluster configuration page.

Step 2 To activate a cluster,

a) Click a cluster from the cluster table.

b) For the desired cluster, click **…** and choose **Activate**.

When you activate the cluster, Cisco SD-WAN Manager establishes a DTLS tunnel with the CSP devices in the cluster, where it connects with the switches through Cisco Colo Manager. When the DTLS tunnel connection is running, a CSP device in the cluster is chosen to host the Cisco Colo Manager. Cisco Colo Manager starts up and Cisco SD-WAN Manager sends global parameter configurations to the CSP devices and Cisco Catalyst 9500 switches. For information about cluster activation progress, see Progress of Cluster Activation. .



Note In Cisco vManage Release 20.7.1 and earlier releases, the Cisco Colo Manager (CCM) and CSP device configuration tasks time out 30 minutes after the tasks are created. In the case of long-running image installation operations, these configuration tasks may time out and fail, while the cluster activation state continues to be in a pending state.

From Cisco vManage Release 20.8.1, the CCM and CSP device configuration tasks time out 30 minutes after the last heartbeat status message that Cisco SD-WAN Manager received from the target devices. With this change, long-running image installation operations do not cause configuration tasks to fail after a predefined interval of time after task creation.

Cluster Configuration

The cluster configuration parameters are:

Login Credentials

1. On the **Cluster Topology** window, click **Add** next to **Credentials**. In the **Credentials** configuration window, enter the following:
   - (Mandatory) Template Name—The template name can contain 128 alphanumeric characters.
   - (Optional) Description—The description can contain 2048 alphanumeric characters.
2. Click **New User**.
   - In the **Name** field, enter the username.
   - In the **Password** field, enter the password and confirm the password in the **Confirm Password** field.
   - In the **Role** drop-down list, select administrators.

3. Click **Add**.

   The new user with username, password, and role with action appears.
4. Click **Save**.

   The login credentials for the new user are added.
5. To cancel the configuration, click **Cancel**.
6. To edit the existing credential for the user, click **Edit** and save the configuration.

Resource Pool

1. On the **Cluster Topology** window, click **Add** next to **Resource Pool**. In the **Resource Pool** configuration window, enter values for the following fields:
   - Name—The name of the IP address pool should contain 128 alphanumeric characters.
   - Description—The description can contain 2048 alphanumeric characters.
2. In the **DTLS Tunnel IP** field, enter the IP addresses to be used for the DTLS tunnel. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 172.16.0.180-172.16.255.190).
3. In the **Service Chain VLAN Pool** field, enter the VLAN numbers to be used for service chains. To enter multiple numbers, separate them by commas. To enter a numeric range, separate the numbers with a hyphen (for example, 1021-2021).

   Consider the following points when entering the VLAN information:

   1002-1005 are the reserved VLAN values, and they shouldn’t be used in the cluster creation VLAN pool.



Note Valid VNF VLAN pool: 1010-2000 and 1003-2000

Invalid: 1002-1005 (shouldn’t be used)



Caution 1002-1005 isn't allowed for configuration. The VLANs tht are allowed should be contiguous.

   Example: Enter data VLAN pool as 1006-2006. Ensure that this VLAN range isn’t used in the Input/Output VLAN during service chain creations.
4. In the **VNF Data Plane IP Pool** field, enter the IP addresses to be used for auto configuring data plane on a VNF interface. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 10.0.0.1-10.0.0.100).
5. In the **VNF Management IP Pool** field, enter the IP addresses to be used for the VNF. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 192.168.30.99-192.168.30.150).

Note These addresses are IP addresses for secure interfaces.

6. In the **Management Subnet Gateway** field, enter the IP address of the gateway to the management network. It enables DNS to exit the cluster.
7. In the **Management Mask** field, enter the mask value for the failover cluster. For example, /24 and not 255.255.255.0
8. In the **Switch PNP Server IP** field, enter the IP address of the switch device.

Note The IP address of the switch is automatically fetched from the management pool, which is the first IP address. You can change it if a different IP address is configured in the DHCP server for the switch.

9. Click **Save**.

Port Connectivity

Table 19: Feature History

Feature Name	Release Information	Description
Flexible Topologies	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1 Cisco NFVIS Release 4.2.1	This feature provides the ability to flexibly insert the NIC cards and interconnect the devices (CSP devices and Catalyst 9500 switches) within the Cloud OnRamp for Colocation cluster. Any CSP ports can be connected to any port on the switches. The Stackwise Virtual Switch Link (SVL) ports can be connected to any port and similarly the uplink ports can be connected to any port on the switches.
Support for SVL Port Configuration on 100G Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1 Cisco NFVIS Release 4.8.1	With this feature, you can configure SVL ports on 100-G Ethernet interfaces of Cisco Catalyst 9500-48Y4C switches, thus ensuring a high level of performance and throughput.

Prerequisites for Configuring SVL and Uplink Ports

- When configuring the SVL and uplink ports, ensure that the port numbers you configure on Cisco SD-WAN Manager match the physically cabled ports.

- Ensure that you assign serial numbers to both the switches. See Create and Activate Clusters.

Configure SVL and Uplink Ports

- On the **Cluster Topology** window, click **Add** next to **Port Connectivity**.

  In the **Port Connectivity** configuration window, both the configured switches appear. Hover over a switch port to view the port number and the port type.

Note For more information about SVL and uplink ports, see Wiring Requirements in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide.

Change Default SVL and Uplink Ports

Before you change the default port number and port type, note the following information about Cisco Catalyst 9500-40X and Cisco Catalyst 9500-48Y4C switches:

- From Cisco vManage Release 20.8.1, you can configure two SVL ports and one Dual-Active Detection (DAD) port when creating a colocation cluster with two Cisco Catalyst 9500-40X switches or two Cisco Catalyst 9500-48Y4C switches.
- To ensure that SVL and DAD ports are configured correctly for Cisco Catalyst 9500-48Y4C switches, note the following information:
  - Configure the SVL ports on same-speed interfaces, that is, either 25-G interfaces or 100-G interfaces. Ensure that both switches have the same configuration.
  - Configure the DAD port only on 25-G interfaces on both switches.
  - In case of an existing cluster, you can change the SVL ports only if it is inactive.
  - A cluster created in releases earlier than Cisco vManage Release 20.8.1 automatically displays two SVL ports and one DAD port after the upgrade to Cisco vManage Release 20.8.1.
- In case of Cisco Catalyst 9500-40X switches, you must configure the SVL and DAD ports on 10-G interfaces on both switches.
- The following are the default SVL, DAD, and uplink ports of Cisco Catalyst 9500 switches:

  Cisco Catalyst 9500-40X

  - SVL ports: Te1/0/38-Te1/0/39, and Te2/0/38-Te2/0/39

    In Cisco vManage Release 20.7.1 and earlier releases, the default SVL ports are Te1/0/38-Te1/0/40 and Te2/0/38-Te2/0/40.
  - DAD ports: Te1/0/40 and Te2/0/40
  - Uplink ports: Te1/0/36, Te2/0/36 (input VLAN handoff), Te1/0/37, and Te2/0/37 (output VLAN handoff)

  Cisco Catalyst 9500-48Y4C

  - SVL ports: Hu1/0/49-Hu1/0/50 and Hu2/0/49-Hu2/0/50

In Cisco vManage Release 20.7.1 and earlier releases, the default SVL ports are Twe1/0/46-Twe1/0/48 and Twe2/0/46-Twe2/0/48.

- DAD ports: Twe1/0/48 and Twe2/0/48
- Uplink ports: Twe1/0/44, Twe2/0/44 (input VLAN handoff), Twe1/0/45, and Twe2/0/45 (output VLAN handoff) for 25-G throughput.

- I, E, and S represent the ingress, egress, and SVL ports, respectively.
- Ensure that the physical cabling is the same as the default configuration, and click **Save**.

To change the default ports when the connectivity is different for SVL and uplink ports, perform the following:

1. If both the switches are using the same ports:
   a. Click a port on a switch that corresponds to a physically connected port.
   b. To add the port configuration to the other switch, check the **Apply change** check box.

   If both the switches aren't using the same ports:
   a. Click a port on **Switch1**.
   b. Choose a port type from the **Port Type** drop-down list.
   c. Click a port on **Switch2** and then choose the port type.
2. To add another port, repeat step 1.
3. Click **Save**.
4. To edit port connectivity information, in the **Cluster Topology** window, click **Edit** next to **Port Connectivity**.



Note You can modify the SVL and uplink ports of a cluster when the cluster hasn't been activated.

5. To reset the ports to default settings, click **Reset**.

The remaining ports (SR-IOV and OVS) on the Cisco CSP devices and the connections with switches are automatically discovered using Link Layer Discovery Protocol (LLDP) when you activate a cluster. You don't need to configure those ports.

Cisco Colo Manager discovers switch neighbor ports and identifies whether all Niantic and Fortville ports are connected. If any port isn't connected, CCM sends notifications to Cisco SD-WAN Manager that you can view in the task view window.

NTP

Optionally, configure the NTP server for the cluster:

1. On the **Cluster Topology** window, click **Add** next to **NTP**. In the **NTP** configuration window, enter the following:

- Template Name—Name of the NTP template should be in alphanumeric characters and the name should contain up to 128 characters.
- Description—The description should be in alphanumeric characters and can be upto 2048 characters.

2. In the **Preferred server** field, enter the IP address of the primary NTP server.
3. In the **Backup server** field, enter the IP address of the secondary NTP server.
4. Click **Save**.

   The NTP servers are added.
5. To cancel the NTP server configuration, click **Cancel**.
6. To edit the NTP server configuration details, click **Edit**.

Syslog Server

Optionally, configure the syslog parameters for the cluster:

1. On the **Cluster Topology** window, click **Add** next to **Syslog**. In the **Syslog** configuration window, enter the following:
   - Template Name—Name of the system template should be in alphanumeric characters and the name can contain up to 128 characters.
   - Description—The description can be up to 2048 characters and can contain only alphanumeric characters.
2. In the **Severity** drop-down list, choose the severity of syslog messages to be logged.
3. To add a new syslog server, click **New Server**.

   Type the IP address of a syslog server.
4. Click **Save**.
5. To cancel the configuration, click **Cancel**.
6. To edit the existing syslog server configuration, click **Edit** and save the configuration.

TACACS Authentication

Table 20: Feature History

Feature Name	Release Information	Description
TACACS Authentication	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to configure the TACACS authentication for users accessing the Cisco CSP and Cisco Catalyst 9500 devices. Authenticating the users using TACACS validates and secures their access to the Cisco CSP and Cisco Catalyst 9500 devices.

The TACACS authentication determines the valid users who can access the Cisco CSP and Cisco Catalyst 9500 devices after a cluster is active.

Points to consider

- By default, the admin users with Role-based access control (RBAC) are authorized to access the Cisco CSP and Cisco Catalyst 9500 devices.
- Do not configure the same user with different passwords when configuring using TACACS and RBAC. If same user with a different password is configured on TACACS and RBAC, the RBAC user and password authentication is used. For information about how to configure RBAC on the devices, see Login Credentials, on page 54.

To authenticate users:

1. To add TACACS server configuration, on the **Cluster Topology** window, click **Other Settings** > **Add** next to **TACACS**.

   To edit TACACS server configuration, in the **Cluster Topology** window, click **Other Settings** > **Edit** next to **TACACS**.

   In the **TACACS** configuration window, enter information about the following:

   - Template Name—The TACACS template name can contain 128 alphanumeric characters.
   - (Optional) Description—The description can contain 2048 alphanumeric characters.

2. To add a new TACACS server, click **+ New TACACS SERVER**.
   - In **Server IP Address**, enter the IPv4 address.

     Use IPv4 addresses for hostnames of TACACS server.
   - In **Secret** enter the password and confirm the password in **Confirm Secret**.

3. Click **Add**

   The new TACACS server details are listed in the **TACACS** configuration window.

Note You can add a maximum of four TACACS servers.

4. To add another TACACS server, repeat step 2 to step 3.

   When authenticating users, if the first TACACS server is not reachable, the next server is verified until all the four servers are verified.

5. Click **Save**.
6. To delete a TACACS server configuration, choose a row from the TACACS server details list and click **Delete** under **Action**.

Note To modify an existing TACACS server information, ensure to delete a TACACS server and then add a new server.

7. To view the TACACS server configuration, in Cisco SD-WAN Manager, click **Configuration** > **Devices**.

   For the desired Cisco CSP device or Cisco Catalyst 9500 switch, click **...** and choose **Running Configuration**.

Backup Server Settings

Points to Consider

- If you don't use an NFS server, Cisco SD-WAN Manager can’t successfully create backup copies of a CSP device for future RMA requirements.
- The NFS server mount location and configurations are same for all the CSP devices in a cluster.
- Don't consider an existing device in a cluster as the replacement CSP device.



Note If a replacement CSP device isn’t available, wait until the device appears in Cisco SD-WAN Manager.

- Don't attach further service chains to a cluster after you identify that a CSP device in the cluster is faulty.
- The backup operation on a CSP device creates backup files containing NFVIS configuration and VMs (if VMs are provisioned on the CSP device). You can use the following information for reference.
  - An automated backup file is generated and is in the format:

    serial_number + "_" + time_stamp + ".bkup"

    For example,

    `WZP22180EW2_2020_06_24T18_07_00.bkup`

  - An internal state model is maintained that specifies the status of the overall backup operation and internal states of each backup component:
    - NFVIS: A configuration backup of the CSP device as an xml file, config.xml.
    - VM_Images: All VNF tar.gz packages in `data/intdatastore/uploads` which are listed individually.
    - VM_Images_Flavors: The VM images such as, img_flvr.img.bkup.
    - Individual tar backups of the VNFs: The files such as, vmbkp.
  - The backup.manifest file contains information of files in the backup package and their checksum for verification during restore operation.

To create backup copies of all CSP devices in a cluster, perform the following steps:

1. On the **Cluster Topology** window, click **Add** next to **Backup**.

   To edit backup server settings, on the **Cluster Topology** window, click **Edit** next to **Backup**

   In the **Backup** configuration window, enter information about the following fields:

   - Mount Name—Enter the name of the NFS mount after mounting an NFS location.

- Storage Space—Enter the disk space in GB.
- Server IP: Enter the IP address of the NFS server.
- Server Path: Enter the folder path of the NFS server such as, `/data/colobackup`
- Backup: Click **Backup** to enable it.
- Time: Set a time for scheduling the backup operation.
- Interval: Choose from the options to schedule a periodic backup process.
  - Daily: The first backup is created a day after the backup configuration is saved on the device, and everyday thereafter.
  - Weekly: The first backup is created seven days after the backup configuration is saved on the device, and every week thereafter.
  - Once: The backup copy is created on a chosen day and it's valid for the entire lifetime of a cluster. You can choose a future calendar date.

2. Click **Save**.
3. To view the status of the previous five backup operations, use the **show hostaction backup status** command. To know about the backup status configuration command, see Backup and Restore NFVIS and VM Configurations. To use this command:
   a. In Cisco SD-WAN Manager, click the **Tools** > **SSH Terminal** screen to start an SSH session with Cisco SD-WAN Manager.
   b. Choose the CSP device.
   c. Enter the username and password for the CSP device and click **Enter** to log in to the CSP device and run the **show hostaction backup status** command.

Restore CSP Device

You can perform the restore operation only by using the CLI on the CSP device that you're restoring.

1. Use the **mount nfs-mount storage** command to mount NFS:

   For more information, see Network File System Support.



Note To access the backup file, the configuration for mounting an NFS file system should match the faulty device. You can view this information from other healthy CSP devices as the NFS mount location and configurations are same for all the CSP devices. To view and capture the information, you can do one of the following:

- In the **Cluster Topology** window, click **Add** next to **Backup**.
- Use the **show running-config** command to view the active configuration that is running on a CSP device.

mount nfs-mount storage { *mount-name* | **server_ip** *server_ip* | **server_path** *server_path* | **storage_space_total_gb** *storage_space_total_gb* | **storage_type** *storage_type* }

For example, `mount nfs-mount storage nfsfs/ server_ip 172.19.199.199 server_path /data/colobackup/ storage_space_total_gb 100.0 storagetype nfs`

2. Restore the backup information on a replacement CSP device using the **hostaction restore** command:

   For example,

   ```
   hostaction restore except-connectivity file-path
   nfs:nfsfs/WZP22180EW2_2020_06_24T18_07_00.bkup
   ```

Note Specify the except-connectivity parameter to retain the connectivity with the NFS server mounted in Step 2.

3. Use the **show hostaction backup status** command to view the status of the previous five backup images and their operational status.

   Also, you can view the backup images from the notifications available on the Cisco SD-WAN Manager **Monitor** > **Logs** > **Events** page.

Note In Cisco vManage Release 20.6.1 and earlier releases, you can view the backup images from the notifications available on the Cisco SD-WAN Manager **Monitor** > **Events** page.

4. Use the **show hostaction restore-status** command on the CSP device to view the status of the overall restore process and each component such as system, image and flavors, VM and so on.
5. To fix any failure after viewing the status, perform a factory default reset of the device.

Note The factory default reset sets the device to default configuration. Therefore, before performing the restore operation from Steps 1-4 on the replacement device, verify that all the restore operation prerequisites are met.

To know more about how to configure the restore operation on CSP devices, see Backup and Restore NFVIS and VM Configurations.

Progress of Cluster Activation

Table 21: Feature History

Feature Name	Release Information	Description
Monitor Cluster Activation Progress	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature displays the cluster activation progress at each step and shows any failures that may occur during the process. The process of activating a cluster takes approximately 30 minutes or longer, and you can monitor the progress using the Cisco SD-WAN Manager task view window and events from the Monitoring page.

To check cluster activation status after activating a cluster, view the progress on the task view window:

Note In Cisco vManage Release 20.7.1 and earlier releases, Cisco Colo Manager bring up and activation progress is reported as part of the CLOUD ONRAMP task. This task shows the seven steps in the Cisco Colo Manager bring up and activation sequence and indicates whether the sequence was successfully completed or not. The Push Feature Template Configuration task shows the status of the RBAC settings configuration push.

Cisco vManage Release 20.8.1, CLOUD ONRAMP task is completed when Cisco SD-WAN Manager receives Cisco Colo Manager Healthy from the target CSP device. The Push Feature Template Configuration task shows the seven steps in the Cisco Colo Manager bring up and activation sequence and indicates whether the sequence was successfully completed or not, along with the status of the RBAC settings configuration push.

Figure 3: Cluster Activation (Cisco vManage Release 20.7.1 and earlier)

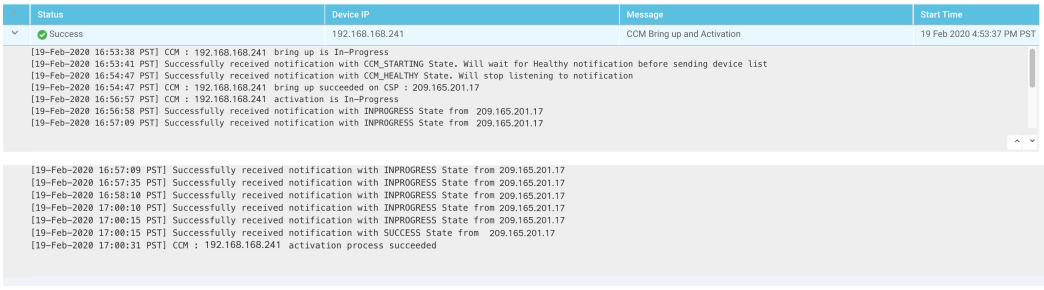


Figure 4: CLOUD ONRAMP Cisco Colo Manager Task (Cisco vManage Release 20.8.1 and later)

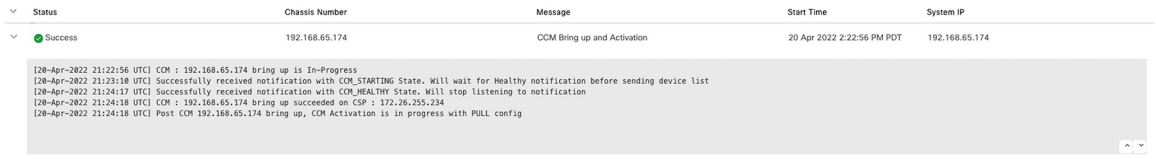
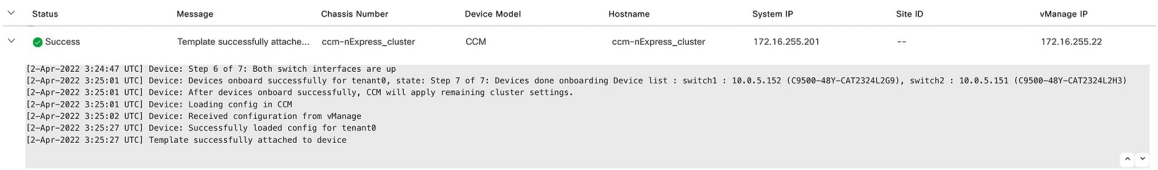


Figure 5: Push Feature Template Configuration Task (Cisco vManage Release 20.8.1 and later)



Perform the following verification steps:

1. To view cluster state and change the state:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**. For the cluster that is goes into a "PENDING" state, click **...**, and choose **Sync**. This action moves a cluster back to an "ACTIVE" state.
   b. To view if a cluster moves back to an "ACTIVE" state, you can view the successful activation for the cluster.
2. To view the service groups, present on CSP devices, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** > **Colocation Cluster**.

Cisco vManage Release 20.6.1 and earlier: To view the service groups present on CSP devices, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network** > **Colocation Clusters**.

Choose a cluster and then choose a CSP device. You can choose and view other CSP devices.

3. To check if cluster is activated from a CSP device:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. View device status of all the CSP devices and ensure that they are in synchronization with Cisco SD-WAN Manager.
   c. View the state of CSP devices and verify that the certificates are installed for CSP devices.



Note If the state of CSP devices doesn't show "cert installed" for more than five minutes after CSP activation through OTP, see .

After a cluster is activated from a CSP device, the Cisco Colo Manager performs the cluster activation tasks on the Cisco NFVIS host.

4. To view if Cisco Colo Manager is enabled for a CSP device,
   a. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

      Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
   b. Click **Colocation Cluster**.

      Cisco vManage Release 20.6.1 and earlier: Click **Colocation Clusters**.

      View whether Cisco Colo Manager is enabled for specific CSP devices.

5. To monitor Cisco Colo Manager health,
   a. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

      Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
   b. Click **Colocation Cluster**.

      Cisco vManage Release 20.6.1and earlier: Click **Colocation Clusters**.

      View whether Cisco Colo Manager is enabled for the desired CSP devices.
   c. For the Cisco Colo Manager-enabled CSP device, click the CSP device.
   d. To view Cisco Colo Manager health, click **Colo Manager**.

If the Cisco Colo Manager status doesn't change to "HEALTHY" after "STARTING", see the "Troubleshoot Cisco Colo Manager Issues" topic in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide .

If the status of Cisco Colo Manager changes to "HEALTHY" after "STARTING" but the status of Cisco Colo Manager shows IN-PROGRESS for more than 20 minutes after the switch configurations are already

complete, see the Switch devices are not calling home to PNP or Cisco Colo Manager topic in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide.

View Cluster

To view cluster configuration, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 2 For the desired cluster, click **...** and choose **View**.

The **Cluster** window displays the switch devices and CSP devices in the cluster and shows the cluster settings that are configured.

You can only view the global parameters of a cluster, configuration of switch devices and CSP devices.

Step 3 Click **Cancel** to return to the **Cluster** window.

Edit Cluster

To modify any existing cluster configuration such as global parameters, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **Edit**.

The **Cluster** window displays the switch devices and CSP devices in the cluster and shows the cluster settings that are configured.

Step 3 In the cluster design window, you can modify some of the global parameters. Based on whether a cluster is in active or inactive state, you can perform the following operations on a cluster:

a. Inactive state:

- Edit all global parameters, and the Resource Pool parameter.
- Add more CSP devices (up to eight).
- Can’t edit the name or serial number of a switch or CSP device. Instead, delete the CSP or switch and add another switch or CSP with a different name and serial number.
- Delete an entire cluster configuration.

b. Active state:

- Edit all global parameters, except the Resource Pool parameter.

Note

You can't change the Resource pool parameter when the cluster is active. However, the only option to change the Resource Pool parameter is to delete the cluster and recreate it with the correct Resource Pool parameter.

- Can’t edit the name or serial number of a switch or CSP device.
- Can’t delete a cluster in an active state.
- Add more CSP devices (up to eight).

Step 4 Click **Save Cluster**.

Add CSP Device to Cluster

You can add and configure the CSP devices using Cisco SD-WAN Manager.

Before you begin

Ensure that the Cisco NFVIS version that you use is same for all the CSP devices in the cluster.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **Add/Delete CSP**.

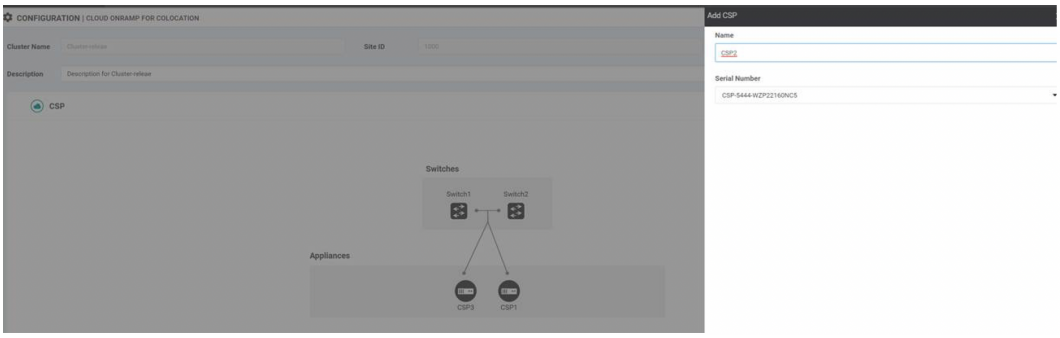
Step 3 To add a CSP device, click **+ Add CSP**. The **Add CSP** dialog box appears. Enter a name and choose the CSP device serial number. Click **Save**.

Step 4 To configure a CSP device, click the CSP icon in the CSP box. The **Edit CSP** dialog box appears. Enter a name and choose the CSP device serial number. Click **Save**.

The name can contain 128 alphanumeric characters.

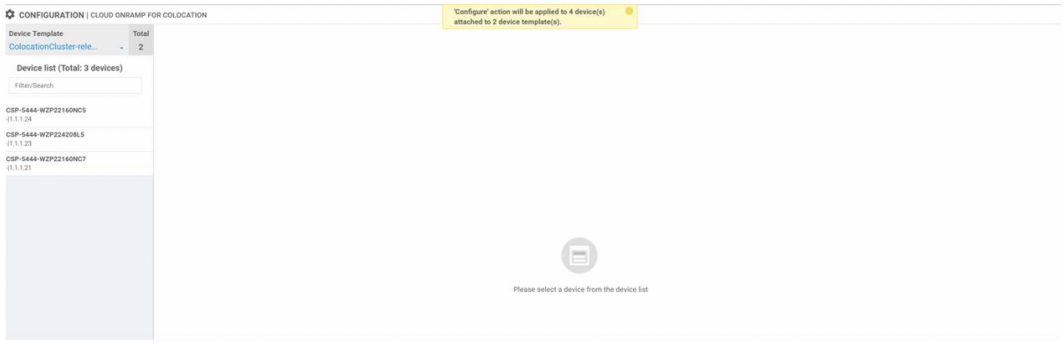
Note
To bring up the CSP devices, ensure that you configure the OTP for the devices.

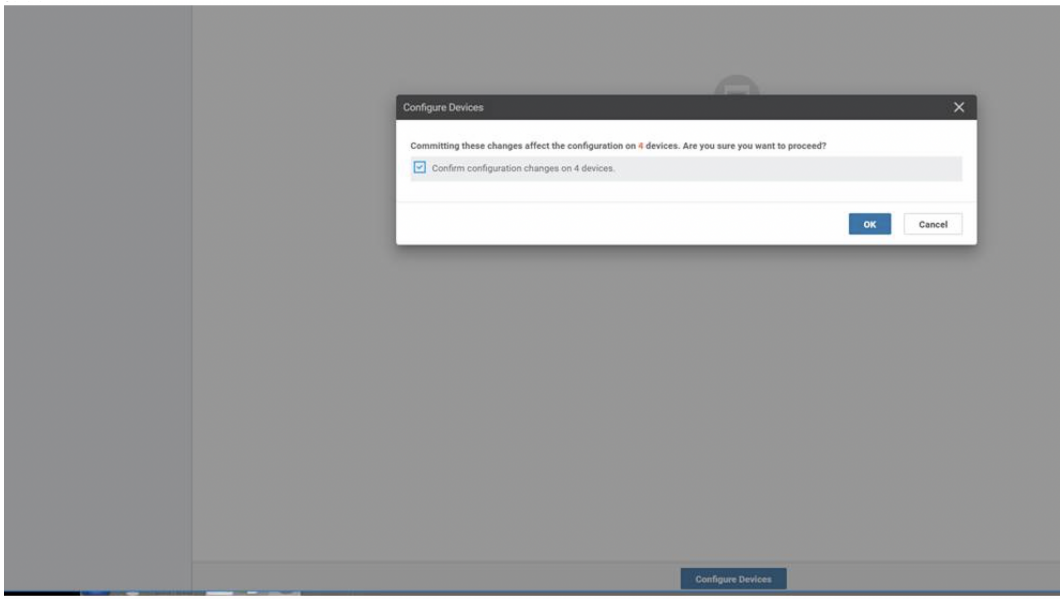
Figure 6: Add a CSP Device



Step 5 Click **Save**.

Step 6 After saving, perform the onscreen configuration instructions as shown in the following images:





Step 7 To check whether the CSP device is added, use the **Task View** window that displays a list of all running tasks.

Delete CSP Devices from Cluster

You can delete CSP devices using Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **Add/Delete CSP**.

Step 3 To delete a CSP device, click the CSP icon from the **Appliances** box.

Step 4 Click **Delete**.

Step 5 Click **Save**.

Step 6 Perform the onscreen instructions to proceed with the deletion as shown in the following images.





Step 7 Reset the CSP devices to factory-default settings.

Step 8 To decommission invalid CSP devices, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 9 For the CSP devices that are in the deactivated cluster, click the **...** and choose **Decommission WAN Edge**.

This action provides new tokens to the devices.

If an HA service chain is deployed on a CSP device that is deleted, the corresponding HA service chains are deleted from the CSP device that hosts the HA instances.

Delete CSP with Cisco Colo Manager

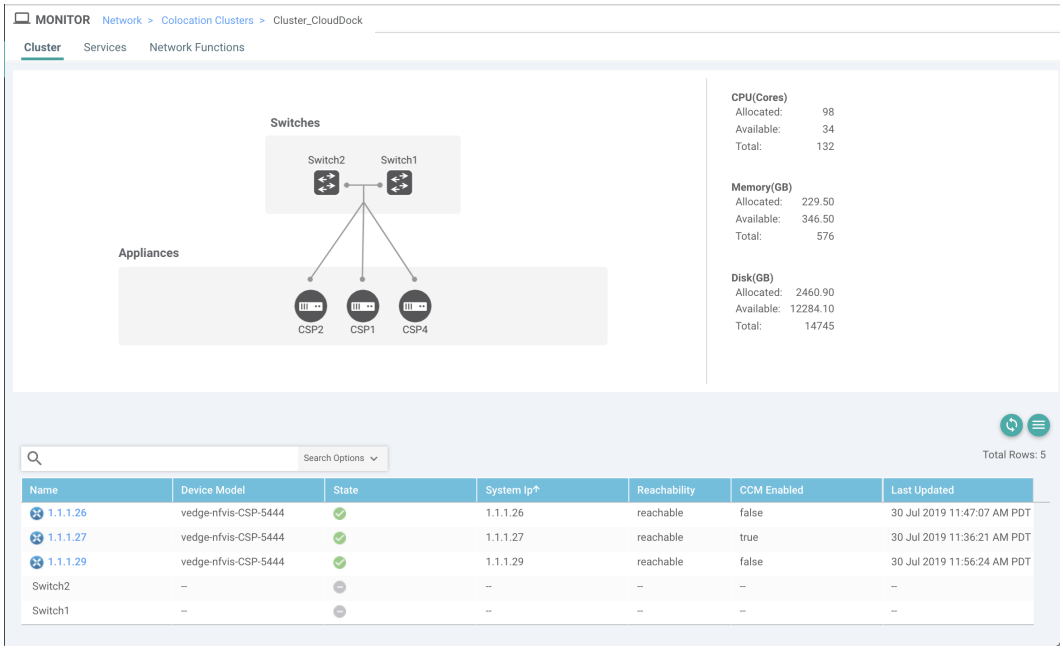
Procedure

Step 1 Determine the CSP device that hosts the Cisco Colo Manager.

Step 2 If **CCM Enabled** is true on a CSP device and you decide to delete this CSP device, for the device, click **...** and choose **Add/Delete CSP**.

From the **Monitor** window, you can view whether Cisco Colo Manager is enabled. The following image shows how where you can view the Cisco Colo Manager status.

Figure 7: CSP Device with Cisco Colo Manager



When the CSP device that you choose to remove from a cluster, runs the service chain monitoring service and Cisco Colo Manager, ensure that you click **Sync** for the cluster. Clicking the sync button starts the service chain health monitoring service on a different CSP device and continues monitoring the existing service chain health.

Ensure that Cisco SD-WAN Manager has control connections to all the CSP devices for a cluster so that it can bring up Cisco Colo Manager instance on another CSP device.

Note
For Cisco vManage Release 20.8.1 and earlier releases, if you delete a CSP device hosting a Cisco Colo Manager instance, you have to add a CSP device to bring up the Cisco Colo Manager instance on one or more of the CSP devices.

After you delete a CSP device with Cisco Colo Manager, the Cisco Colo Manager instance starts on another CSP device on the cluster.

Note The service chain monitoring is disabled until the Cisco Colo Manager instance doesn't start in any of the remaining CSP devices.

Replace Cisco CSP Devices After RMA

SUMMARY STEPS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**
2. For the desired cluster, click **...** and choose **RMA**.
3. Do the following in the **RMA** dialog box:

DETAILED STEPS

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **RMA**.

Step 3 Do the following in the **RMA** dialog box:

a) Select Appliance: Choose a CSP device that you want to replace.

All CSP devices in a specific colocation cluster are displayed in the format, CSP Name-<Serial Number>.

b) Choose a serial number for a new CSP device from the drop-down list.

c) Click **Save**.

After saving, you can view the configuration.

Return of Materials of Cisco CSP Devices

Table 22: Feature History

Feature Name	Release Information	Description
RMA Support for Cisco CSP Devices	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to replace a faulty CSP device by creating backup copies of the device, and then restoring the replacement device to a state it was in before the replacement. The VMs running in HA mode operate uninterrupted with continuous flow of traffic during device replacement.

You can now create backup copies and restore NFVIS configurations and VMs.

Points to Consider

- You can use Network File Storage (NFS) servers to create regular backup copies of the CSP devices.
- If you’re using an external NFS server for the backup operation, ensure that you maintain and clean the NFS directory regularly. This maintenance ensures that the NFS server has sufficient space for the incoming backup packages.
- If you don’t use NFS servers, don't configure the backup server settings using Cisco SD-WAN Manager. However, if you're not configuring the backup server settings, you can't restore the replacement device. You can use delete CSP to remove the faulty device, add a new CSP device, and then start provisioning the service chains onto the added CSP device.

RMA Process for Cisco CSP Devices

Ensure that you perform the Return of Materials (RMA) process in the following order:

1. Create a backup copy of all the CSP devices in a cluster using Cisco SD-WAN Manager. See Backup Server Settings, on page 61.



Note During CSP device replacement, create a backup copy of the device in the NFS server when creating a cluster using Cisco SD-WAN Manager. Perform one of the following if you're bringing up a cluster or editing an existing cluster.

- Bring up a colocation cluster: At the time of cluster creation and activation, provide information about the NFS storage server and backup intervals. If the backup task fails on a CSP device, the device returns an error, but the cluster activation continues. Ensure that you update the cluster after addressing the failure and wait for a successful cluster activation.
- Edit a colocation cluster: For an existing active cluster, edit the cluster and provide information about the NFS storage server and backup intervals.

2. Contact Cisco Technical Support to get a replacement CSP device. See Cisco Cloud Services Platform 5000 Hardware Installation Guide for more information about replacing a CSP device.
3. Rewire the replacement Cisco CSP device with the Cisco Catalyst 9500 switches to move the wiring of the faulty device to the replacement device.
4. Verify that the Cisco CSP ISO image running on the replacement device is the same that was running on the faulty device.
5. Restore the replacement device using CLI.

Prerequisites and Restrictions for Backup and Restore of CSP Devices

Prerequisites

Backup Operation

- The connectivity to the NFS server from CSP devices should be established before configuring the backup server settings using Cisco SD-WAN Manager.
- The backup directory on the NFS server should have write permission.
- The external NFS server should be available, reachable, and maintained. The maintenance of the external NFS server requires you to check the available storage space and network reachability regularly.
- The schedule for the backup operation should be synced with the local date and time on the CSP device.

Restore Operation

- The replacement device should have the same resources as the faulty device. These resources are, Cisco NFVIS image version, CPU, memory and storage as the faulty CSP device.
- The connectivity between the replacement device and switch ports should be same as the faulty device and switches.
- The PNIC wiring of the replacement device should match the faulty device on the Catalyst 9500 switches.

  For example,

If slot-1/port-1 (eth1-1) on the faulty device is connected to switch-1 and port, 1/0/1, then connect slot-1/port-1 (eth1-1) of the replacement device to the same switch port, such as switch-1 and port, 1/0/1.

- The onboarding of the replacement device should be completed using the PnP process for CSP devices.
- To prevent the loss of backup access during the restore operation, the configuration for mounting an NFS server to access the backup package should match the configuration on the faulty device.

  You can view configuration information from other CSP devices as the NFS mount location and configurations are same for all the CSP devices. To view the active configuration that is running on a healthy CSP device, use the **show running-config** command. Use this active configuration information when creating a mount point during the restore operation.

  For example,

```
nfvis# show running-config mount
mount nfs-mount storage nfsfs/
storagetype            nfs
storage_space_total_gb 123.0
server_ip              172.19.199.199
server_path            /data/colobackup/
!
```

- The authentication of the replacement device with the Cisco SD-WAN Control Components using the OTP process should be completed after restoring the replacement device.



Note Use the **request activate chassis-number** *chassis-serial-number* **token** *token-number* command to authenticate a device by logging in to Cisco NFVIS.

- The replacement device shouldn't have any configuration other than the configuration of the faulty device.

Restrictions

Backup Operation

- The periodic backup operation doesn't start during the upgrade of a CSP device.
- If the NFS folder path isn't available on the NFS server, the backup operation doesn't start.
- Only one backup operation can occur at a specific time.
- The backup operation fails if the available disk space on the NFS server is less than the combined size of the VM export size and tar.gz VM packages.
- The backup device information can only be restored on a replacement CSP device and not on any existing device that is already part of the cluster.
- The NFS mount configurations can’t be updated after they are configured for a CSP device. To update, delete the NFS configuration and reapply an updated configuration to the NFS server and reconfigure the backup schedule. Perform this update when the backup operation isn't in progress.

Restore Operation

- Only one restore operation can occur at a specific time.
- If a backup file doesn’t exist in the NFS server, the restore operation doesn't start.

- The restore operation isn't supported when you convert a cluster from a single tenant mode to multitenant mode, and conversely.

Remove Cluster

To decommission an entire cluster from Cisco SD-WAN Manager, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

Step 2 Verify the **Validate** column for the CSP devices that you wish to delete, and click **Invalid**.

Step 3 For the invalid devices, click **Send to Controllers**.

Step 4 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 5 For the cluster that has invalid CSP devices, click **...** and choose **Deactivate**.

If the cluster is attached to one or more service groups, a message appears that displays the service chains hosting the VMs that are running on the CSP device and whether you can continue with the cluster deletion. However, although you confirm the deletion of a cluster, you're not allowed to remove the cluster without detaching the service groups that are hosted on this CSP device. If the cluster isn't attached to any service group, a message appears that gets a confirmation from you about the cluster deletion.

Note
You can delete the cluster, if necessary, or can keep it in deactivated state.

Step 6 To delete the cluster, choose **Delete**.

Step 7 Click **Cancel** if you don't wish to delete the cluster.

Step 8 To decommission invalid devices, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 9 For the devices that are in the deactivated cluster, click **...** and choose **Decommission WAN Edge**.

This action provides new tokens to your devices.

Step 10 Reset the devices to the factory default by using the command:

factory-default-reset all

Step 11 Log into Cisco NFVIS by using **admin** as the login name and **Admin123#** as the default password.

Step 12 Reset switch configuration and reboot switches. See the Troubleshooting chapter in Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide.

Reactivate Cluster

To add new CSP devices or when CSP devices are considered for RMA process, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Locate the devices that are in a deactivated cluster.

Step 3 Get new token from Cisco SD-WAN Manager for the devices.

Step 4 Log into Cisco NFVIS using **admin** as the login name and **Admin123#** as the default password.

Step 5 Use the **request activate chassis-number** *chassis-serial-number* **token** *token-number* command.

Step 6 Use Cisco SD-WAN Manager to configure the colocation devices and activate the cluster. See Create and Activate Clusters, on page 52.

If you've deleted the cluster, recreate and then activate it.

Step 7 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**. Locate and verify status of the colocation devices.

Step 8 For the desired device that should be valid, click **Valid**.

Step 9 For the valid devices, click **Send to Controllers**.

Manage Service Groups

A service group consists of one or more service chains. You can configure a service group using Cisco SD-WAN Manager. A service chain is the structure of a network service, and consists of a set of linked network functions.

Create Service Chain in a Service Group

A service group consists of one or more service chains.

Table 23: Feature History

Feature Name	Release Information	Feature Description
Monitor Service Chain Health	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster.

Procedure

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

a) Click **Service Group** and click **Create Service Group**. Enter the service group name, description, and colocation group.

The service group name can contain 128 alphanumeric characters.

The service group description can contain 2048 alphanumeric characters.

For a multitenant cluster, choose a colocation group or a tenant from the drop-down list. For a single-tenant cluster, the colocation group **admin** is chosen by default.

b) Click **Add Service Chain**.
c) In the **Add Service Chain** dialog box, enter the following information:

Table 24: Add Service Chain Information

Field	Description
Name	The service chain name can contain 128 alphanumeric characters.
Description	The service chain description can contain alphanumeric 2048 characters.
Bandwidth	The service chain bandwidth is in Mbps. The default bandwidth is 10 Mbps and you can configure a maximum bandwidth of 5 Gbps.
Input Handoff VLANS and Output Handoff VLANS	The Input VLAN handoff and output VLAN handoff can be comma-separated values (10, 20), or a range from 10–20.
Monitoring	A toggle button that allows you to enable or disable service chain health monitoring. The service chain health monitoring is a periodic monitoring service that checks health of a service chain data path and reports the overall service chain health status. By default, the monitoring service is disabled. A service chain with subinterfaces such as, SCHM (Service Chain Health Monitoring Service) can only monitor the service chain including the first VLAN from the subinterface VLAN list. The service chain monitoring reports status based on end-to-end connectivity. Therefore, ensure that you take care of the routing and return traffic path, with attention to the Cisco Catalyst SD-WAN service chains for better results. **Note** • Ensure that you provide input and output monitoring IP addresses from input and output handoff subnets. However, if the first and last VNF devices are VPN terminated, you don't need to provide input and output monitoring IP addresses. For example, if the network function isn't VPN terminated, the input monitoring IP can be 192.0.2.1/24 from the inbound subnet, 192.0.2.0/24. The inbound subnet connects to the first network function and the output monitoring IP can be, 203.0.113.11/24 that comes from outbound subnet, 203.0.113.0/24 of the last network function of a service chain. • If the first or last VNF firewall in a service chain is in transparent mode, you can't monitor these service chains.
Service Chain	A topology to choose from the service chain drop-down list. For a service chain topology, you can choose any of the validated service chains such as, Router - Firewall - Router, Firewall, Firewall - Router. See the Validated Service Chains topic in Cisco Catalyst SD-WAN Cloud OnRamp Colocation Solution Guide. You can also create a customized service chain. See Create Custom Service Chain, on page 84.

d) In the **Add Service Chain** dialog box, click **Add**.

Based on the service chain configuration information, a graphical representation of the service group with all the service chains and the VNFs automatically appear in the design view window. A VNF or PNF appears with a "V" or "P" around the circumference for a virtual a physical network function. It shows all the configured service chains within each service group. A check mark next to the service chain indicates that the service chain configuration is complete.

After you activate a cluster, attach it with the service group and enable monitoring service for the service chain, when you bring up the CSP device where CCM is running. Cisco SD-WAN Manager chooses the same CSP device to start the monitoring service. The monitoring service monitors all service chains periodically in a round robin fashion by setting the monitoring interval to 30 minutes. See Monitor Cloud OnRamp Colocation Clusters, on page 108.

e) In the design view window, to configure a VNF, click a VNF in the service chain.
The **Configure VNF** dialog box appears.

f) Configure the VNF with the following information and perform the actions, as appropriate:

Note
The following fields are available from Cisco vManage Release 20.7.1:

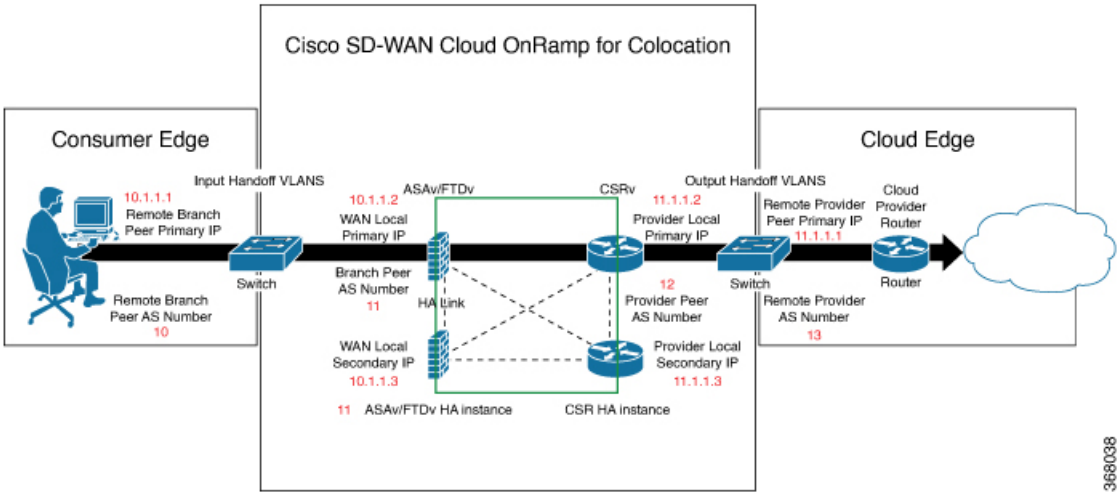
- **Disk Image/Image Package (Select File)**
- **Disk Image/Image Package (Filter by Tag, Name and Version)**
- **Scaffold File (Select File)**
- **Scaffold File (Filter by Tag, Name and Version)**

Table 25: VNF Properties of Router and Firewall

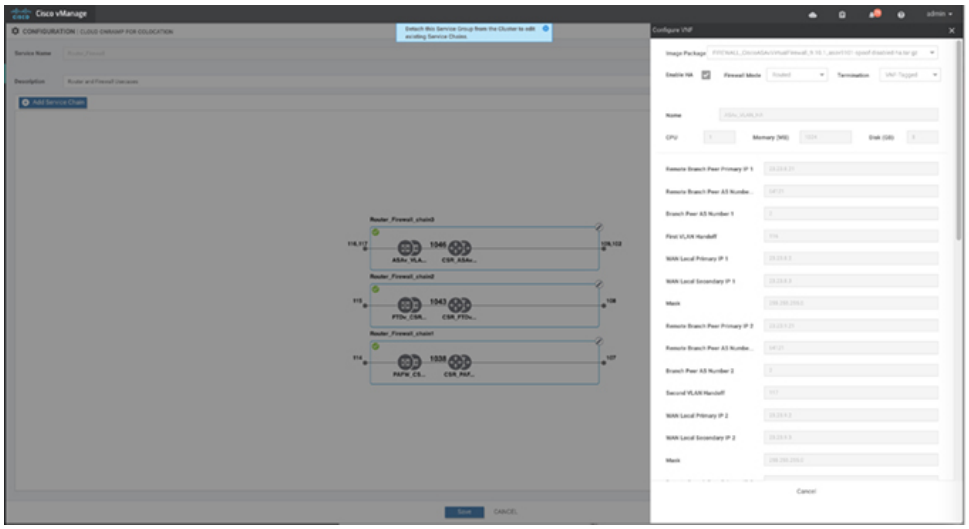
Field	Description
Image Package	Choose a router, firewall package.
Disk Image/Image Package (Select File)	Choose a tar.gz package or a qcow2 image file.
Disk Image/Image Package (Filter by Tag, Name and Version)	(Optional) Filter an image or a package file based on the name, version, and tags that you specified when uploading a VNF image.
Scaffold File (Select File)	Choose a scaffold file. **Note** • This field is mandatory if a qcow2 image file has been chosen. It is optional if a tar.gz package has been chosen. • If you choose both a tar.gz package and a scaffold file, then all image properties and system properties from the scaffold file override the image properties and system properties, including the Day-0 configuration files, specified in the tar.gz package.
Scaffold File (Filter by Tag, Name and Version)	(Optional) Filter a scaffold file based on the name, version, and tags that you specified when uploading a VNF image.

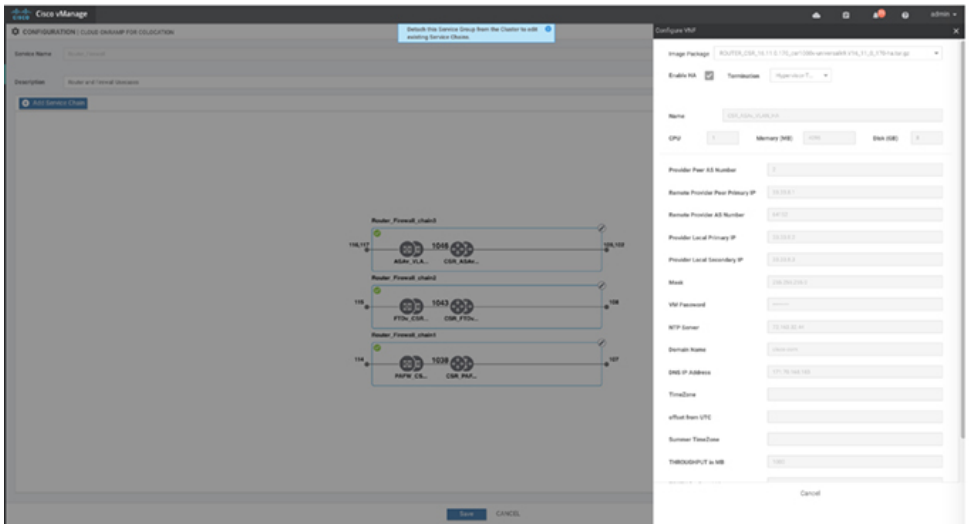
Field	Description
Click **Fetch VNF Properties**. The available information for the image is displayed in the **Configure VNF** dialog box.	
Name	VNF image name
CPU	(Optional) Specifies the number of virtual CPUs that are required for a VNF. The default value is 1 vCPU.
Memory	(Optional) Specifies the maximum primary memory in MB that the VNF can use. The default value is 1024 MB.
Disk	(Optional) Specifies disk in GB required for the VM. The default value is 8 GB.
A dialog box with any custom tokenized variables from Day-0 that requires your input appears. Provide the values.	

In the following image, all IP addresses, VLAN, and autonomous system within the green box are system-specific information that is generated from the VLAN, IP pools provided for the cluster. The information is automatically added into the Day-0 configurations of VMs.



The following images are a sample configuration for VNF IP addresses and autonomous system numbers, in Cisco SD-WAN Manager.





If you're using a multitenant cluster and a comanged scenario, configure theCisco Catalyst SD-WAN VM by entering the values for the following fields and the remaining fields, as required for the service chain design:

Note
To join the tenant overlay network, the provider should provide correct values for the following fields.

Field	Description
Serial Number	The authorized serial number of a Cisco Catalyst SD-WAN device. The service provider can get the device serial number from the tenant before creating the service chain.
OTP	The OTP of the Cisco Catalyst SD-WAN device that is available after authenticating it with Cisco SD-WAN Control Components. The service provider can get the OTP for the corresponding serial number from the tenant before creating the service chain.

Field	Description
Site Id	The identifier of the site in the tenant Cisco Catalyst SD-WAN overlay network domain in which the Cisco Catalyst SD-WAN device resides, such as a branch, campus, or data center. The service provider can get the site Id from the tenant before creating the service chain.
Tenant ORG Name	The tenant organization name that is included in the Certificate Signing Request (CSR). The service provider can get the organization name from the tenant before creating the service chain.
System IP connect to Tenant	The IP address to connect to the tenant overlay network. The service provider can get the IP address from the tenant before creating the service chain.
Tenant vBond IP	The IP address of the tenant Cisco SD-WAN Validator. The service provider can get the Cisco SD-WAN Validator IP address from the tenant before creating the service chain.

For edge VMs such as first and last VM in a service chain, you must provide the following addresses as they peer with a branch router and the provider router.

Table 26: VNF Options for First VM in Service Chain

Field	Mandatory or Optional	Description
Firewall Mode	Mandatory	Choose Routed or Transparent mode. **Note** Firewall mode is applicable to firewall VMs only.
Enable HA	Optional	Enable HA mode for the VNF.

Termination	Mandatory	Choose one of the following modes:
		• L3 mode selection with subinterfaces that are in trunk mode
		`<type>selection</type> <val help="L3 Mode With Sub-interfaces(Trunked)" display="VNF-Tagged">vlan</val>`
		• L3 mode with IPSEC termination from a consumer-side and rerouted to the provider gateway
		`<val help="L3 Mode With IPSEC Termination From Consumer and Routed to Provider GW" display="Tunneled">vpn</val>`
		• L3 mode with access mode (nontrunk mode)
		`<val help="L3 Mode In Access Mode (Non-Trunked)" display="Hypervisor-Tagged">routed</val>`

g) Click **Configure**. The service chain is configured with the VNF configuration.
h) To add another service chain, repeat the procedure from Steps b-g.
i) Click **Save**.

The new service group appears in a table under the **Service Group**. To view the status of the service chains that are monitored, use the **Task View** window, which displays a list of all running tasks along with the total number of successes and failures. To determine the service chain health status, use the **show system:system status** command on the CSP device that has service chain health monitoring enabled.

QoS on Service Chains

Table 27: Feature History

Feature Name	Release Information	Description
QoS on Service Chains	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature classifies the network traffic based on the Layer 2 virtual local-area network (VLAN) identification number. The QoS policy allows you to limit the bandwidth available for each service chain by applying traffic policing on bidirectional traffic. The bidirectional traffic is the ingress side that connects Cisco Catalyst 9500-40X switches to the consumer and egress side that connects to the provider.

Prerequisites

- Ensure that you use the Quality of Service (QoS) traffic policing on service chains that do not have shared VNF and PNF devices.

Note You cannot apply QoS policy on service chains with shared VNF devices where input and output VLANs are same for multiple service chains.

- Ensure that you use the following versions of software for QoS traffic policing:

Software	Release
Cisco NFVIS Cloud OnRamp for Colocation	4.1.1 and later
Catalyst 9500-40X	16.12.1 and later

The QoS policing policy is applied on the network traffic based on the following workflow:

1. Cisco SD-WAN Manager saves the bandwidth, input, or output VLAN information to VNF and PNF devices. To provide bandwidth and VLAN information, see Create Service Chain in a Service Group, on page 75.
2. CCM saves the bandwidth, input, or output VLAN values information to the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches.
3. CCM creates corresponding class-maps and policy-maps in Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches based on VLAN match criteria.
4. CCM applies input service-policy on the ingress and egress ports.

Note From Cisco vManage Release 20.7.1, the QoS traffic policy on service chains is not supported for Cisco Catalyst 9500 switches.

- If an active cluster is upgraded to Cisco vManage Release 20.7.1 and CSPs 4.7.1, and if there are service chains provisioned prior to upgrade, the QoS configuration will be removed from switches during the upgrade automatically.
- When new service chains are provisioned in Cisco vManage Release 20.7.1, the QoS policy will not be configured on switches.
- Similarly, new clusters created in Cisco vManage Release 20.7.1 will not configure QoS configuration for service chains on switches.

Clone Service Groups

Table 28: Feature History

Feature Name	Release Information	Description
Clone Service Groups in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to create copies of service groups for different RBAC users, without having to enter the same configuration information multiple times. By cloning a service group, you can easily create service chains by leveraging the stored service chain templates.

When you clone or create copies of service chains, remember the following:

- Cisco SD-WAN Manager copies all configuration information of a service group to a cloned service group regardless of whether the cloned service group is attached to a cluster.
- Verify the CSV file and ensure that configuration information has a matching service group name during CSV file upload. Otherwise, an unmatched service group name can result in an error message during CSV file upload.
- To get an updated list of service group configuration values, always download service group configuration properties from the service group design view.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 Click **Service Group**.
The service group configuration page appears and all the service groups are displayed.

Step 3 For the desired service group, click **...** and choose **Clone Service Group**.

A clone of the original service group appears in the service group design view. Note the following points:

- By default, the cloned service group name and VM names are suffixed with a unique string.
- To view any VM configuration, click a VM in service chains.
- Cisco SD-WAN Manager marks the service chains that require configuration as **Unconfigured**, next to the edit button of the service chain.

Step 4 Modify the service group name, if required. Provide a description for the service group.

Step 5 To configure a service chain, use one of the following methods:

- Click the edit button for a service chain, enter the values, and then click **Save**.
- Download the configuration values from a CSV file, modify the values, upload the file, and then click **Save**. See Steps 6, 7, 8 on how to download, modify, and upload a CSV file.

The cloned service group appears on the service group configuration page. You can now download the updated service group configuration values.

Step 6 To download the cloned service group configuration values, do one of the following:

Note
The download and upload of a CSV file is supported for creating, editing, and cloning of the service groups that aren't attached to a cluster.

- On the service group configuration page, click a cloned service group, click **More Actions** to the right of the service group, and choose **Download Properties (CSV)**.
- In the service group design view, click **Download CSV** in the upper right corner of the screen.

Cisco SD-WAN Manager downloads all configuration values of the service group to an Excel file in CSV format. The CSV file can consist of multiple service groups and each row represents configuration values for one service group. To add more rows to the CSV file, copy service group configuration values from existing CSV files and paste them in this file.

For example, ServiceGroup1_Clone1 that has two service chains with one VM in each of the service chains is represented in a single row.

Note
In the Excel file, the headers and their representation in the service chain design view is as follows:

- sc1/name represents the name of the first service chain.
- sc1/vm1/name represents the name of the first VNF in the first service chain.
- sc2/name represents the name of the second service chain.
- sc2/vm2/name represents the name of the second VNF in the second service chain.

Step 7 To modify service group configuration values, do one of the following:

- To modify the service group configuration in the design view, click a cloned service group from the service group configuration page.

  Click any VM in service chains to modify the configuration values, and then click **Save**.
- To modify the service group configuration using the downloaded Excel file, enter the configuration values in the Excel file manually. Save the Excel file in CSV format.

Step 8 To upload a CSV file that includes all the configuration values of a service group, click a service group in the service group configuration page, and then click **Upload CSV** from the right corner of the screen.

Click **Browse** to choose a CSV file, and then click **Upload**.

You can view the updated values displayed for the service group configuration.

Note
You can use the same CSV file to add configuration values for multiple service groups. But, you can update configuration values for a specific service group only, when uploading a CSV file using Cisco SD-WAN Manager.

Step 9 To know the representation of service group configuration properties in the CSV file and Cisco SD-WAN Manager design view, click a service group from the service group configuration page.

Click **Show Mapping Names**.

A text appears next to all the VMs in the service chains. Cisco SD-WAN Manager displays this text after mapping it with the configuration properties in the CSV file.

Create Custom Service Chain

You can customize service chains,

- By including extra VNFs or add other VNF types.
- By creating new VNF sequence that isn't part of the predefined service chains.

Procedure

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 75.

Step 2 In the **Add Service Chain** dialog box, enter the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, monitoring health information of a service chain, and service chain configuration. Click **Add**.

For the service chain configuration, choose **Create Custom** from the drop-down. An empty service chain in the design view window is available.

Step 3 To add a VNF such as a router, load balancer, firewall, and others, click a VNF icon and drag the icon to its proper location within the service group box. After adding all required VNFs and forming the VNF service chain, configure each of the VNFs. Click a VNF in the service group box. The **Configure VNF** dialog box appears. Enter the following parameters:

a) Choose the software image to load from the **Disk Image/Image Package** (**Select File**) drop-down list.

Note
You can select a qcow2 image file from Cisco vManage Release 20.7.1.

b) Choose a scaffold file from the **Scaffold File** (**Select File**) drop-down list if you have chosen a qcow2 image file.

Note
This option is available from Cisco vManage Release 20.7.1.

c) Optionally, filter an image, a package file, or a scaffold file based on the name, version, and tags that you specified when uploading a VNF image.

Note
This option is available from Cisco vManage Release 20.7.1.

d) Click **Fetch VNF Properties**.
e) In the **Name** field, enter a name of the VNF.
f) In the **CPU** field, enter the number of virtual CPUs required for the VNF.
g) In the **Memory** field, enter the amount of memory in megabytes to be allocated for the VNF.
h) In the **Disk** field, enter the amount of memory for storage in gigabytes to be allocated for the VNF.
i) Enter VNF-specific parameters, as required.

Note
These VNF details are the custom variables that are required for Day-0 operations of the VNF.

j) Click **Configure**.
k) To delete the VNF or cancel the VNF configuration, click **Delete** or **Cancel** respectively.

The customized service chains are added to a service group.



Note You can customize a VNF sequence with only up to four VNFs in a service chain.

Custom Service Chain with Shared PNF Devices

You can customize service chains by adding supported PNF devices.



Caution Ensure that you don't share PNF devices across colocation clusters. A PNF device can be shared across service chains, or across service groups. However, a PNF device can now be shared only across a single cluster.

Table 29: Feature History

Feature Name	Release Information	Feature Description
Manage PNF Devices in Service Chains	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain.

Before you begin

For more information about validated physical network functions, see the Validated Physical Network Functions topic in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide.

To create a customized service chain by adding a router or firewall to an existing service chain, ensure that you note the following points:

- If a PNF device needs to be managed byCisco SD-WAN Manager, ensure that the serial number is already available in Cisco SD-WAN Manager, which can then be available for selection during PNF configuration.
- The FTD device can be in any position in a service chain.
- An ASR 1000 Series Aggregation Services Routers can only be in the first and last position in a service chain.
- PNF devices can be added across service chains and service groups.
- PNF devices can be shared across service groups. They can be shared across service groups by entering the same serial numbers.
- PNF devices can be shared across a single colocation cluster, and can't be shared across multiple colocation clusters.

Procedure

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 75.

Step 2 In the **Add Service Chain** dialog box, enter the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, monitoring health information of a service chain, and service chain configuration. Click **Add**.

For the service chain configuration, choose **Create Custom** from the drop-down list. An empty service chain in the design view window is available. At the left, a set of VNF devices and PNF devices that you can add into the service chain appears. The 'V' in the circumference of VNF devices represents a VNF and 'P' in the circumference of PNF devices represent a PNF.

Note
Ensure that you choose the **Create Custom** option for creating service chains by sharing PNF devices.

Step 3 To add a PNF such as physical routers, physical firewalls in a service chain, click the required PNF icon, and drag the icon to the proper location within the service chain box.

After adding all required PNF devices, configure each of them.

a) Click a PNF device in the service chain box.

The **Configure PNF** dialog box appears. To configure a PNF, enter the following parameters:

b) Check **HA Enabled** if HA is enabled for the PNF device.

c) If the PNF is HA enabled, ensure that you add the HA serial number in **HA Serial**.

If the PNF device is FTD, enter the following information.

1. In the **Name** field, enter a name of the PNF.
2. Choose Routed or Transparent mode as the **Firewall Mode**.

3. In the **PNF Serial** field, enter the serial number of the PNF device.

If the PNF device is ASR 1000 Series Aggregation Services Routers, enter the following information.

1. Check the **vManaged** check box if the device is managed by Cisco SD-WAN Manager.
2. Click **Fetch Properties**.
3. In the **Name** field, enter a name of the PNF.
4. In the **PNF Serial** field, enter the serial number of the PNF device.

d) Click **Configure**.

Step 4 To add service chains and share PNF devices, repeat from Step 2.

Step 5 To edit an existing PNF configuration, click the PNF.

Step 6 In the **Share NF To** drop-down list, choose the service chains with which the PNF should be shared.

After a PNF is shared, if you hover over a PNF, the respective shared PNF devices are highlighted in blue color. However, the PNFs from different service groups aren't highlighted in blue color. After you choose an NF to be shared, a blue color rim appears. If the same PNF is shared across multiple service chains, it can be used in different positions by dragging and placing the PNF icons in a specific position.

Figure 8: Single PNF in a Service Chain

The following image shows a service chain that consists of a single PNF, Ftd_Pnf (not shared with other service chains).

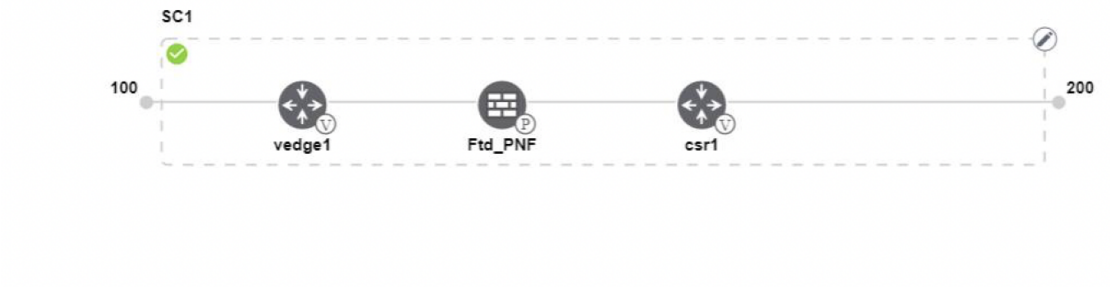


Figure 9: Two PNF Devices in Service Chains

The following image shows service chains that consist of two PNFs, FTdv_PNF shared across service chain 1 (SC1) and service chain 2 (SC2) and ASR_PNF (non-shared).

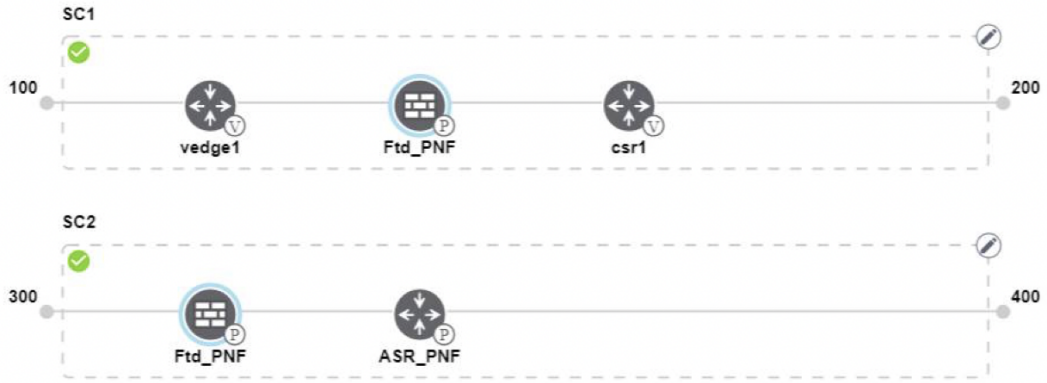
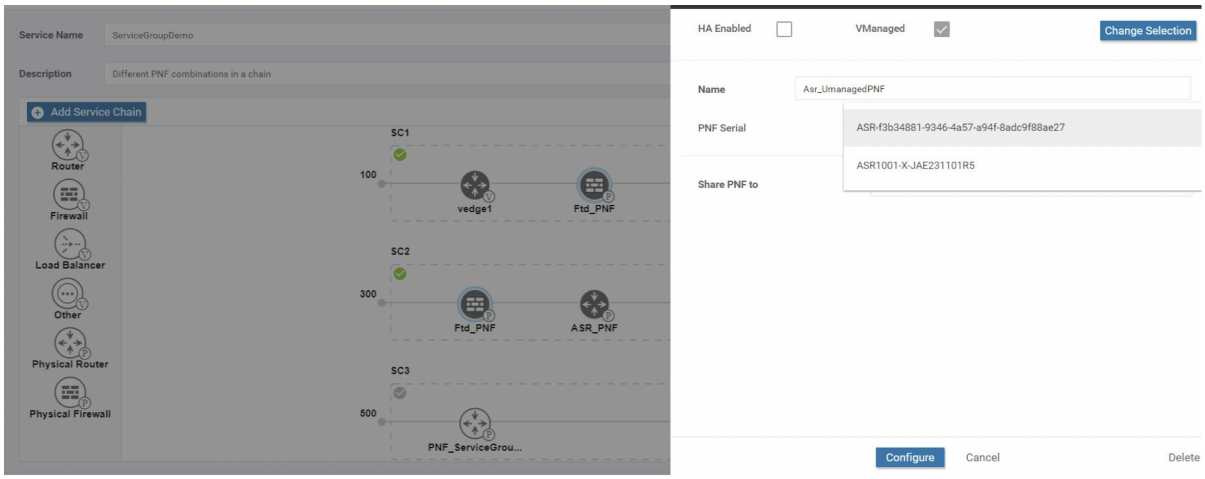


Figure 10: Three PNF Devices in Service Chains

The following image shows service chains that consist of three PNF devices in two different positions along with Cisco SD-WAN Manager configuration.



Step 7 To delete or cancel a Network Function configuration, click **Delete** or **Cancel** respectively.

You must attach the service groups to a colocation cluster. After attaching service groups that contain PNF devices, the PNF configuration isn't automatically pushed to the PNF devices unlike VNF devices. Instead, you must manually configure the PNF device by noting configuration that is generated on the Monitor window. The VLANs must be also configured on the Cisco Catalyst 9500-40X switch devices. See the ASR 1000 Series Aggregation Services Routers Configuration Guides and Cisco Firepower Threat Defense Configuration Guides for more information about the specific PNF configuration.

Custom Service Chain with Shared VNF Devices

You can customize service chains by including supported VNF devices.

Table 30: Feature History

Feature Name	Release Information	Feature Description
Share VNF Devices Across Service Chains	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation.

Before you begin

Ensure that you note the following points about sharing VNF devices:

- You can share only the first, last, or both first and last VNF devices in a service chain.
- You can share a VNF with a minimum of one more service chain and maximum up to five service chains.
- Each service chain can have a maximum of up to four VNF devices in a service chain.
- You can share VNF devices only in the same service group.

Procedure

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 75.

Step 2 In the **Add Service Chain** dialog box, enter the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, monitoring health information of a service chain, and service chain configuration. Click **Add**.

For the service chain configuration, choose **Create Custom** from the drop-down list. An empty service chain in the design view window is available. At the left, a set of VNF devices and PNF devices that you can add into the service chain appears. The 'V' in the circumference of VNF devices represents a VNF and 'P' in the circumference of PNF devices represent a PNF.

Note
Ensure that you choose the **Create Custom** option for creating a shared VNF package.

Step 3 To add a VNF such as a router, load balancer, firewall, and others, click a VNF icon from the left panel, and drag the icon to a proper location within the service chain box.

After adding all required VNF devices, configure each of them.

a) Click a VNF in the service chain box.

The **Configure VNF** dialog box appears. To configure VNF, enter the following parameters:

b) From the **Image Package** drop-down list, choose the software image to load.

To create a customized VNF package from Cisco SD-WAN Manager, see Create Customized VNF Image, on page 95.

c) Click **Fetch VNF Properties**.
d) In the **Name** field, enter a name of the VNF.
e) In the **CPU** field, enter the number of virtual CPUs required for the VNF.

f) In the **Memory** field, enter the amount of memory in megabytes to be allocated for the VNF.
g) In the **Disk** field, enter the amount of memory for storage in gigabytes to be allocated for the VNF.
h) Enter VNF-specific parameters, as required. See Create Service Chain in a Service Group, on page 75 for more information about VNF-specific properties.

These VNF-specific parameters are the custom user variables that are required for Day-0 operations of a VNF.

Note
Ensure that you enter the values of the user variables if they are defined as mandatory, and the system variables are automatically set by Cisco SD-WAN Manager.

i) Click **Configure**.

Step 4 To share VNF devices, repeat from Step 2.

Step 5 To edit an existing VNF configuration, click the VNF.

Step 6 Scroll down the VNF configuration to find the **Share NF To** field. From the **Share NF To** drop-down list, choose the service chains with which the VNF should be shared.

After a VNF is shared, if you hover over a VNF, the specific shared VNF devices are highlighted in blue color. After you choose an NF to be shared, a blue rim appears on it.

Step 7 To delete a VNF or cancel the VNF configuration, click **Delete** or **Cancel** respectively.

You must attach service groups to a cluster.

View Service Groups

To view service groups, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 Click **Service Group**.

Step 3 For the desired service group, click **...** and choose **View**.

You can view the service chains in the design window.

Edit Service Groups

Before attaching a service group with a cluster, you can edit all parameters. After attaching a service group with a cluster, you can only edit monitoring configuration parameters. Also, after attaching a service group, you can only add new service chains but not edit or attach a service chain. Hence, ensure that you detach a service group from a cluster before editing an existing service chain. To edit and delete a service group, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 2 Click **Service Group**.

Step 3 For the desired service group, click **...** and choose **Edit**.

Step 4 To modify either service chain configuration or modify a VNF configuration, click a router or firewall VNF icon.

Step 5 To add new service chains, click **Add Service Chain**.

Attach or Detach a Service Group in a Cluster

To complete the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation configuration, you must attach service groups to a cluster. To attach or detach a service group to and from a cluster, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 2 Click **...** adjacent to the corresponding cluster and choose **Attach Service Groups**.

Step 3 In the **Attach Service Groups** dialog box, choose one or more service groups in **Available Service Groups** and click **Add** to move the selected groups to **Selected Service Groups**.

Step 4 Click **Attach**.

Step 5 To detach a service group from a cluster, click **...** adjacent to the corresponding cluster and choose **Detach Service Groups**.

You can’t attach or detach a single service chain within a service group.

Step 6 In the **Config Preview** window that is displayed, click **Cancel** to cancel the attach or detach task.

Note

.

Step 7 To verify if service groups are attached or detached, you can view the status using Cisco SD-WAN Manager. Note the following points:

- If the status of the tasks in the **Task View** window is displayed as **FAILURE** or in **PENDING** for a long duration, see the "Troubleshoot Service Chain Issues" topic in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution guide.
- If a Cisco Colo Manager task fails, see the "Troubleshoot Cisco Colo Manager Issues" topic in the Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide.

If a colocation cluster moves to **PENDING** state, for a cluster, click **...**, and choose **Sync**. This action moves the cluster back to **ACTIVE** state. The **Sync** option keeps Cisco SD-WAN Manager synchronized with the colocation devices.

Manage VM Catalog and Repository

Table 31: Feature History

Feature Name	Release Information	Description
Support for Cisco VM Image Upload in qcow2 Format	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to upload a virtual machine image to Cisco SD-WAN Manager in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.

Cisco SD-WAN Manager supports uploading a prepackaged Cisco virtual machine image, tar.gz, or an image in qcow2 format. It is mandatory to upload a scaffold file if you choose a qcow2 image file. Similarly, you can now select either an image package file or a qcow2 image file with a scaffold file when configuring a Virtual Network Function (VNF) during service chain creation.

A scaffold file contains the following components:

- VNF metadata (image_properties.xml)
- System-generated variables from cluster resource pools for service chaining (system_generated_propeties.xml)
- Tokenized Day-0 configuration files
- Package manifest file (package.mf)

Alternatively, you can package the VM image by providing a root disk image in any of the supported formats (qcow2). Use the linux command-line NFVIS VM packaging tool, **nfvpt.py** to package the qcow2 or alternatively create a customized VM image using Cisco SD-WAN Manager. See Create Customized VNF Image, on page 95.

A VM is SR-IOV capable means sriov_supported is set to true in image_properties.xml in the vm package *.tar.gz. Also, the service chain network is automatically connected to SR-IOV network. If sriov_supported is set to false, an OVS network is created on the data port channel. It's attached to VM VNICs for service chaining by using the OVS network. For the Cloud OnRamp for Colocation solution, a VM uses homogeneous type of network in service chains. This type of network means it's either OVS or SR-IOV, and not a combination of SR-IOV and OVS.

Only two data VNICs are attached to any VM–one for inbound traffic and the other for outbound traffic. If more than two data interfaces are required, use subinterfaces configuration within the VM. The VM packages are stored in the VM catalog.

Note Each VM type such as firewall can have multiple VM images that are uploaded to Cisco SD-WAN Manager from same or different vendors and added to a catalog. Also, different versions that are based on the release of the same VM can be added to a catalog. However, ensure that the VM name is unique.

The Cisco VM image format can be bundled as *.tar.gz and can include:

- Root disk images to boot the VM.
- Package manifest for checksum validation of the file listing in the package.
- Image properties file in XML format that lists the VM meta data.
- (Optional) Day-0 configuration, other files that are required to bootstrap the VM.
- (Optional) HA Day-0 configuration if VM supports stateful HA.
- System-generated properties file in XML format that lists the VM system properties.

VM images can be hosted on both HTTP server local repository that Cisco SD-WAN Manager hosts or on the remote server.

If VM is in Cisco NFVIS supported VM package format such as, tar.gz, Cisco SD-WAN Manager performs all the processing and you can provide variable key and values during VNF provisioning.



Note Cisco SD-WAN Manager manages the Cisco VNFs, and the Day-1 and Day-N configurations within VNF aren't supported for other VNFs. See the Cisco NFVIS Configuration Guide, VM Image Packaging for more information about VM package format and content, and samples on image_properties.xml and manifest (package.mf).

To upload multiple packages for the same VM, same version, communication manager (CM) type, ensure that one of the three values (name, version, VNF type) are different. Then, you can repackage the VM *.tar.gz to be uploaded.

Upload VNF Images

The VNF images are stored in the Cisco SD-WAN Manager software repository. These VNF images are referenced during service chain deployment, and then they are pushed to Cisco NFVIS during service chain attachment.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 To add a prepackaged VNF image, click **Virtual Images**, and then click **Upload Virtual Image**.

Step 3 Choose the location to store the virtual image.

- To store the virtual image on the local Cisco SD-WAN Manager server and download it to CSP devices over a control plane connection, click **Manager**. The **Upload VNF's Package to Manager** dialog box appears.
  - **a.** Drag and drop the virtual image file or the qcow2 image file to the dialog box or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server. For example, CSR.tar.gz, ASAv.tar.gz, or ABC.qcow2
  - **b.** If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

c. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

- Description of the image
- Version number of the image
- Checksum
- Hash algorithm

You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

Note
- It is mandatory to upload a scaffold file if you choose a qcow2 image file.
- The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

d. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it available for installing on the CSP devices.

- To store the image on a remote Cisco SD-WAN Manager server and then download it to CSP devices, click **Remote Server - Manager**. The **Upload VNF's Package to Remote Server-Manager** dialog box appears.

a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on Cisco SD-WAN Manager server that is in the management VPN (typically, VPN 512).

b. Drag and drop the virtual image file or the qcow2 image file to the dialog box, or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server.

c. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

d. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

- Description of the image
- Version number of the image
- Checksum
- Hash algorithm

You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

Note
- It is mandatory to upload a scaffold file if you choose a qcow2 image file.
- The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

e. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

You can have multiple VNF entries such as a firewall from same or from different vendors. Also, you can add different versions of VNF that are based on the release of the same VNF. However, ensure that the VNF name is unique.

Create Customized VNF Image

Before you begin

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.
- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

- Root disk image for a VNF–qcow2
- Day-0 configuration files–system and tokenized custom variables
- VM configuration–CPU, memory, disk, NICs
- HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link.
- Additional Storage–If more storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .

Step 2 Click **Virtual Images** > **Add Custom VNF Package**.

Step 3 Configure the VNF with the following VNF package properties and click **Save**.

Table 32: VNF Package Properties

Field	Mandatory or Optional	Description
Package Name	Mandatory	The filename of the target VNF package. It's the Cisco NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Cisco VNFs or third-party VNFs.

Field	Mandatory or Optional	Description
Name	Mandatory	Name of the VNF image.
Version	Optional	Version number of a program.
Type	Mandatory	Type of VNF to choose. Supported VNF types are: Router, Firewall, Load Balancer, and Other.

Step 4 To package a VM qcow2 image, click **File Upload**, and browse to choose a qcow2 image file.

Step 5 To choose a bootstrap configuration file for VNF, if any, click **Day 0 Configuration** and click **File Upload** to browse and choose the file.

Include the following Day-0 configuration properties:

Table 33: Day-0 Configuration

Field	Mandatory or Optional	Description
Mount	Mandatory	The path where the bootstrap file gets mounted.
Parseable	Mandatory	A Day-0 configuration file can be parsed or not. Options are: **Enable** or **Disable**. By default, **Enable** is chosen.
High Availability	Mandatory	High availability for a Day-0 configuration file to choose. Supported values are: Standalone, HA Primary, HA Secondary.

Note
If any bootstrap configuration is required for a VNF, create a *bootstrap-config* or a *day0-config* file.

Step 6 To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** next to the desired Day-0 configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

Note
The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see the Custom Packaging Details for Shared VNF topic and additional references in Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide for the list of system variables that must be added for different VNF types..

a) To add a system variable, in the **CLI configuration** dialog box, select, and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
b) Choose a system variable from the **Variable Name** drop-down list, and click **Done**. The highlighted property is replaced by the system variable name.

c) To add a custom variable, in the **CLI configuration** dialog box, choose and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
d) Enter the custom variable name and choose a type from **Type** drop-down list.
e) To set the custom variable attribute, do the following:
   - To ensure that the custom variable is mandatory when creating a service chain, click **Type** next to **Mandatory**.
   - To ensure that a VNF includes both primary and secondary day-0 files, click **Type** next to **Common**.
f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

Step 7 To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an extra qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

Note
Ensure that you don't combine ephemeral disks and storage volumes when uploading extra VM images.

Step 8 To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

Table 34: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	The disk size that is required for the VM operation. If the size unit is GiB, the maximum disk size can be 256 GiB.
Size Unit	Mandatory	Choose size unit. The supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. By default, disk is chosen.
Location	Optional	The location of the disk or CD-ROM. By default, it's local.
Format	Optional	Choose a disk image format. The supported formats are: qcow2, raw, and vmdk. By default, it's raw.
Bus	Optional	Choose a value from the drop-down list. The supported values for a bus are: virtio, scsi, and ide. By default, it's virtio.

Step 9 To add VNF image properties, expand **Image Properties** and enter the following image information.

Table 35: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Enable or disable SR-IOV support. By default, it's enabled.
Monitored	Mandatory	VM health monitoring for those VMs that you can bootstrap. The options are: enable or disable. By default, it's enabled.
Bootup Time	Mandatory	The monitoring timeout period for a monitored VM. By default, it's 600 seconds.
Serial Console	Optional	The serial console that is supported or not. The options are: enable or disable. By default, it's disabled.
Privileged Mode	Optional	Allows special features like promiscuous mode and snooping. The options are: enable or disable. By default, it's disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. The options are: enable or disable. By default, it's enabled.

Step 10 To add VM resource requirements, expand **Resource Requirements** and enter the following information.

Table 36: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	The CPUs supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	The RAM supported by a VM. The RAM can range 2–32.
Disk Size	Mandatory	The disk size in GB supported by a VM. The disk size can range 4–256.

Field	Mandatory or Optional	Description
Max number of VNICs	Optional	The maximum number of VNICs allowed for a VM. The number of VNICs can from range 8–32 and by default, the value is 8.
Management VNIC ID	Mandatory	The management VNIC ID corresponding to the management interface. The valid range is from 0 to maximum number of VNICs.
Number of Management VNICs ID	Mandatory	The number of VNICs.
High Availability VNIC ID	Mandatory	The VNIC IDs where high availability is enabled. The valid range is from 0–maximum number of VNICs. It shouldn't conflict with management VNIC Id. By default, the value is 1.
Number of High Availability VNICs ID	Mandatory	The maximum number of VNIC IDs where high availability is enabled. The valid range is 0–(maximum number of VNICs-number of management VNICs-2) and by default, the value is 1.

Step 11 To add day-0 configuration drive options, expand **Day 0 Configuration Drive options** and enter the following information.

Table 37: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	The volume label of the Day-0 configuration drive. The options are: V1 or V2. By default, the option is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.
Init Drive	Optional	The Day-0 configuration file as a disk when mounted. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. The supported values for a bus are: virtio, scsi, and ide. By default, it's ide.

The Software Repository table displays the customized VNF image, and image is available for choosing when creating a custom service chain.

View VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**.

Step 3 To filter the search results, use the filter option in the search bar.

The Software Version column provides the version of the software image.

The Software Location column indicates where the software images are stored. Software images can be stored either in the repository on the Cisco SD-WAN Manager server or in a repository in a remote location.

The **Version Type Name** column provides the type of firewall.

The **Available Files** column lists the names of the VNF image files.

The **Update On** column displays when the software image was added to the repository.

Step 4 For the desired VNF image, click **...** and choose **Show Info**.

Delete VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**. The images in the repository are displayed in a table.

Step 3 For the desired image, click **...** and choose **Delete**.

Note If you're downloading a VNF image to a device, you can’t delete the VNF image until the download process completes.

Note If the VNF image is referenced by a service chain, it can’t be deleted.

Upgrade Cisco NFVIS Using Cisco SD-WAN Manager

To upload and upgrade Cisco NFVIS, the upgrade image must be available as an archive file that can be uploaded to the Cisco SD-WAN Manager repository using Cisco SD-WAN Manager. After you upload the Cisco NFVIS image, the upgraded image can be applied to a CSP device by using the **Software Upgrade** window in Cisco SD-WAN Manager. You can perform the following tasks when upgrading Cisco NFVIS software using Cisco SD-WAN Manager:

- Upload Cisco NFVIS upgrade image. See Upload NFVIS Upgrade Image, on page 101.
- Upgrade a CSP device with the uploaded image. See Upgrade a CSP Device with a Cisco NFVIS Upgrade Image, on page 101.
- View the upgrade status for the CSP device by clicking the **Tasks** icon located in the Cisco SD-WAN Manager toolbar.

Upload NFVIS Upgrade Image

Procedure

Step 1 Download the Cisco NFVIS upgrade image from a prescribed location to your local system. You can also download the software image to an FTP server in your network.

Step 2 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .

Step 3 Click **Add New Software** > **Remote Server/Remote Server - Manager**.

You can either store the software image on a remote file server, on a remote Cisco SD-WAN Manager server, or on a Cisco SD-WAN Manager server.

Cisco SD-WAN Manager server: Saves software images on a local Cisco SD-WAN Manager server.

Remote server: Saves the URL pointing to the location of the software image and can be accessed using an FTP or HTTP URL.

Remote Cisco SD-WAN Manager server: Saves software images on a remote Cisco SD-WAN Manager server and location of the remote Cisco SD-WAN Manager server is stored in the local Cisco SD-WAN Manager server.

Step 4 To add the image to the software repository, browse and choose the Cisco NFVIS upgrade image that you had downloaded in Step1.

Step 5 Click **Add**|**Upload**.

The Software Repository table displays the added NFVIS upgrade image, and it's available for installing on the CSP devices. See the Manage Software Upgrade and Repository topic in the Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide.

Upgrade a CSP Device with a Cisco NFVIS Upgrade Image

Before you begin

Ensure that the Cisco NFVIS software versions are the files that have `.nfvispkg` extension.

Procedure

Step 1 From theCisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** > **WAN Edge**.

Step 2 Check one or more CSP device check boxes for the devices you want to choose.

Step 3 Click **Upgrade**. The **Software Upgrade** dialog box appears.

Step 4 Choose the Cisco NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

Step 5 To automatically upgrade and activate with the new Cisco NFVIS software version and reboot the CSP device, check the **Activate and Reboot** check box.

If you don't check the **Activate and Reboot** check box, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new Cisco NFVIS software version by choosing the device again and clicking the **Activate** button in the **Software Upgrade** window.

Step 6 Click **Upgrade**.

The **Task View** window displays a list of all running tasks along with total number of successes and failures. The window periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status window by clicking the **Task View** icon located in the Cisco SD-WAN Manager toolbar.

Note
If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happens in a sequence.

Note
The **Set the Default Software Version** option isn't available for the Cisco NFVIS images.

The CSP device reboots and the new NFVIS version is activated on the device. This reboot happens during the **Activate** phase. The activation can either happen immediately after upgrade if you check the **Activate and Reboot** check box, or by manually clicking **Activate** after choosing the CSP device again.

To verify if CSP device has rebooted and is running, use the task view window. Cisco SD-WAN Manager polls your entire network every 90 seconds up to 30 times and shows the status on th task view window.



Note You can delete a Cisco NFVIS software image from a CSP device if the image version isn't the active version that is running on the device.

Supported Upgrade Scenarios and Recommended Connections

The following are the various upgrade scenarios and cluster states that determine the use of prescriptive or flexible connections.

Table 38: Supported Connections

Cisco SD-WAN Manager	Cisco NFVIS	Cluster State	Supported Connections
Upgrade from Releases 19.3 or 20.1.1.1 to Release 20.3.1	Upgrade from Releases 3.12 or 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Releases 19.3 or 20.1.1.1	Use prescriptive connections
Use the latest Release, 20.3.1	Use the latest Release, 4.2.1	Cluster created and active in Cisco vManage Release 20.3.1	Can use prescriptive or flexible connections
Upgrade from Release 20.1.1.1 to Release 20.3.1	Upgrade from Release 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Release 20.1.1.1	Use prescriptive connections
Upgrade from Release 20.1.1.1 to Release 20.3.1	Upgrade from Release 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Release 20.1.1.1. To add a new Cisco CSP device after upgrade, see Add a Cisco CSP device to the cluster after upgrading Cisco vManage and Cisco NFVIS.	Use prescriptive connections
Upgrade from Release 20.1.1.1 to Release 20.3.1	Upgrade from Release 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Cisco vManage Release 20.3.1	Can use prescriptive or flexible connections

Add Cisco CSP Device to Cluster After Upgrading Cisco SD-WAN Manager and Cisco NFVIS

To add a Cisco CSP device to a cluster if the cluster was created before upgrading Cisco SD-WAN Manager to Release 20.3.1, perform the following steps:

1. Connect the cables for the newly added Cisco CSP device according to prescriptive connections.
2. Upgrade Cisco NFVIS to Release 4.2.1
3. Use the following commands on the newly added Cisco CSP device by logging into Cisco NFVIS:
   - **request csp-prescriptive-mode**

     Requests the newly added Cisco CSP device to run in prescriptive mode.
   - **request activate chassis-number** *chassis number* **token** *serial number*

     Activates the Cisco CSP device

     Example

     ```
     request activate chassis-number 71591a3b-7d52-24d4-234b-58e5f4ad0646 token
     e0b6f073220d85ad32445e30de88a739
     ```

Recommendations Prior to Updating a Cluster

- To use an already active cluster when you upgrade to the latest release of the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, ensure that you upgrade Cisco SD-WAN Manager and Cisco NFVIS to the latest releases.
- To create a new cluster when you upgrade to the latest release of the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, ensure that you upgrade Cisco SD-WAN Manager and Cisco NFVIS to the latest releases for flexible connections.

Monitor Operational Status of Cloud OnRamp for Colocation Devices from Cisco Catalyst SD-WAN Manager

Monitoring colocation devices is the process of reviewing and analyzing a device, such as Cloud Services Platform (CSP) devices and Cisco Colo Manager for health, inventory, availability, and other operation-related processes. You can also monitor the components of CSP devices such as CPU, memory, fan, temperature, and so on. For more information about theCisco SD-WAN Manager Monitoring screens, see the Cisco Catalyst SD-WAN Configuration Guides configuration guides.

All notifications are sent to the Cisco SD-WAN Manager notification stream. To use the notification stream command, see Cisco Catalyst SD-WAN Command Reference.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco SD-WAN Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

If Cisco SD-WAN Manager can't reach the CSP devices and Cisco Colo Manager cannot reach the switches, the CSP devices and Cisco Colo Manager are shown as unreachable.

Step 2 Click a CSP device or a switch from the list by clicking the hostname.

By default, the VNF Status window appears.

Step 3 Click **Select Device** and to filter the search results for devices, use the Filter option in the search bar.

The following are the categories of information about the device that are displayed:

- VNF Status—Displays performance specifications, required resources, and component network functions for each VNF See View Information About VNFs , on page 106.
- Interface—Displays Interface status and statistics See the "View Interfaces" topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Control Connections—Displays status and statistics for control connections See the View Control Connections topic in the Cisco Catalyst SD-WAN Configuration Guides.
- System Status—Displays reboot and crash information, hardware component status, and CPU and memory usage. See the View Control Connections topic in the Cisco Catalyst SD-WAN Configuration Guides.

- Cisco Colo Manager—Displays Cisco Colo Manager health status See View Cisco Colo Manager Health, on page 105.
- Events—Displays latest system logging (syslog) events. See the View Events topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Troubleshooting—Displays information about pings and traceroute traffic connectivity tools See the Troubleshoot a Device topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Real Time—Displays real-time device information for feature-specific operational commands. See the View Real-Time Data topic in the Cisco Catalyst SD-WAN Configuration Guides.

Step 4 To monitor colocation clusters, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and click **Colocation Cluster**.

Cisco vManage Release 20.6.1 and earlier: To monitor colocation clusters, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network** and click **Colocation Clusters**.

Step 5 Click the desired cluster name. See Monitor Cloud OnRamp Colocation Clusters, on page 108 for more information.

View Cisco Colo Manager Health

You can view Cisco Colo Manager (CCM) health for a device, CCM host system IP, CCM IP, and CCM state. Reviewing this information can help you to determine which VNF to use when you're designing a network service chain. To view information about VNFs, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco SD-WAN Manager Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

The information of all devices is displayed in a tabular format.

Step 2 Click a CSP device from the table.

Step 3 From the left pane, click **Colo Manager**.

The right pane displays information about the memory usage, CPU usage, uptime, and so on, of the Cisco Colo Manager.

View Information About VNFs

Table 39: Feature History

Feature Name	Release Information	Description
VNF States and Color Codes	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature allows you to determine the state of a deployed VM using color codes, which you can view on the **Monitor** > **Devices** page. These color codes help you make decisions on creating service chains based on the state of the VM.

Table 40: Feature History

Feature Name	Release Information	Description
Network Utilization Charts for SR-IOV Enabled NICs and OVS Switch	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature allows you to view network utilization charts of VM VNICs connected to both SR-IOV enabled NICs and OVS switch. These charts help you determine if the VM utilization is optimal to create service chains.

You can view performance specifications and required resources for each VNF. Reviewing this information can help you to determine which VNF to use when you're designing a network service. To view information about VNFs, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Cisco SD-WAN Manager displays the VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

Step 2 Click a CSP device from the table.

Step 3 From the left pane, click **VNF Status**.

Step 4 From the table, click the VNF name. Cisco SD-WAN Manager displays information about the specific VNF. You can click the network utilization, CPU utilization, memory utilization, and disk utilization to monitor the VNF resources utilization.

The following VNF information is displayed:

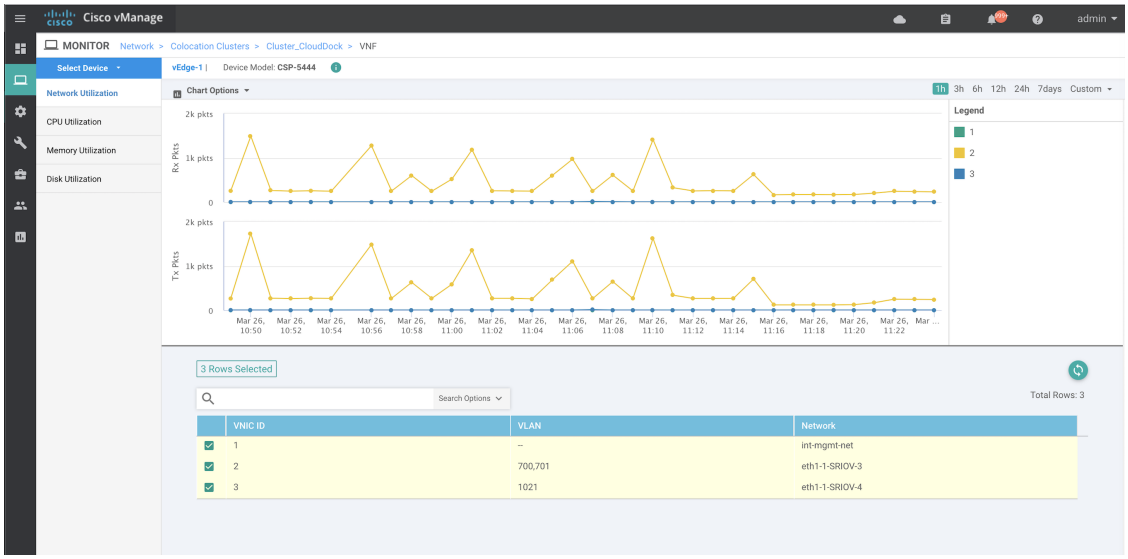
Table 41: VNF Information

Chart options bar	VNF information in graphical format	VNF information in color coded format
• Chart Options drop-down—Click Chart Options drop-down list to select the type of data to display. • Time periods—Click either a predefined time period, or a custom time period for which to display data.	Choose a VNF from the **Select Device** drop-down list to display information for the VNF.	The VNFs are shown in specific colors based on the following operational status of the VNF life cycle: • Green—VNF is healthy, deployed, and successfully booted up. • Red—VNF deployment or any other operation fails, or VNF stops. • Yellow—VNF is transitioning from one state to another.

The right pane displays the following:

- Filter criteria
- VNF table that lists information about all VNFs or VMs. By default, the first six VNFs are selected. The network utilization charts for VNICs connected to SR-IOV enabled NICs and OVS switch are displayed.

Figure 11: VNF Information



The graphical display plots information for the VNFs that you have selected by checking the check box.

- Click the check box at the left to select and deselect VNFs. You can select and display information for a maximum of six VNFs at a time.
- To change the sort order of a column, click the column title.

Monitor Cloud OnRamp Colocation Clusters

Table 42: Feature History

Feature Name	Release Information	Description
Network Assurance –VNFs: Stop/Start/Restart	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature provides the capability to stop, start, or restart VNFs on Cisco CSP devices from the **Colocation Cluster** tab. You can easily perform the operations on VNFs using Cisco SD-WAN Manager.

You can view the cluster information and their health states. Reviewing this information can help you to determine which Cisco CSP device is responsible for hosting each VNF in a service chain. To view information about a cluster, perform the following steps:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 To monitor clusters, click **Colocation Cluster**.

Cisco vManage Release 20.6.1 and earlier: Click **Colocation Clusters**.

All clusters with relevant information are displayed in a tabular format. Click a cluster name. You can monitor cluster by clicking **Config. View** and **Port Level View**.

- **Config. View**: The primary part of the window displays the CSP devices and switch devices that form the cluster. In the right pane, you can view the cluster information such as the available and total CPU resources, available and allocated memory, and so on, based on colocation size.

  The detail part of the window contains:

  - Search: To filter the search results, use the Filter option in the search bar.
  - A table that lists information about all devices in a cluster (Cisco CSP devices, PNFs, and switches).

    Click a Cisco CSP device. VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, number of CPUs, memory consumption, and other core parameters that define performance of a network service chain. See View Information About VNFs , on page 106 .

    To start, stop, or reboot a VNF, for the desired VNF, click **...** and choose one of the following operations:

    - **Start**.
    - **Stop**.
    - **Restart**.

Note

Ensure that service chain provisioning is complete and VMs are deployed, before issuing start, stop, restart operations on any of the VNFs in the service chain.

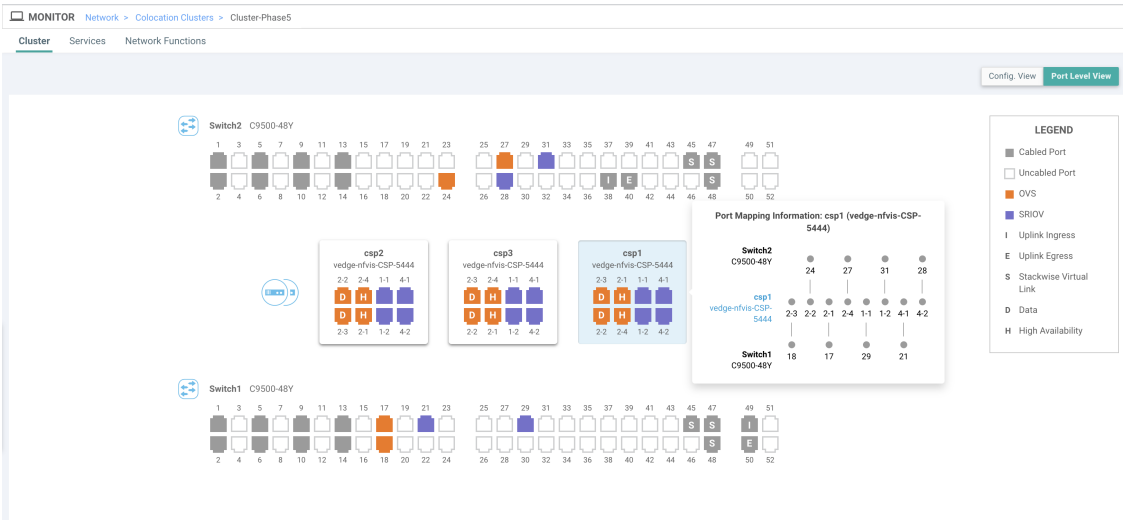
After you choose an operation on a VNF, wait until the operation is complete before you issue another operation. You can view the progress of an operation from the **Task View** window.

- **Port Level View**: After you activate the cluster, to view the port connectivity details, click **Port Level View**.

  You can view detailed port connectivity information for the switches and CSP devices in a color coded format based on the SR-IOV and OVS modes.

  To view the mapping of ports between the Catalyst 9500 switches and CSP devices, click or hover over a CSP device.

Figure 12: Monitor Port Connectivity Details of a Cluster



Step 3 Click **Services**.

Here, you can view the following:

- Complete information of a service chain. The first two columns display the name and description of the service chain in the service group and the remaining columns mention about the VNF, PNF statuses, monitoring service enablement, and the overall health of a service chain. You can also view the colocation user group associated with a service chain. The various health statuses and their representations are:
  - Healthy—An up arrow in green. A service chain is in 'Healthy' status when all the VNF, PNF devices are running and are in healthy state. Ensure that you configure the routing and policy correctly.
  - Unhealthy—A down arrow in red. If one of the VNFs or PNFs are in unhealthy state, the service chain is reported to be in 'Unhealthy' status. For example, after deploying a service chain, if one of the network function IP address changes on the WAN or LAN side, or the firewall policy isn't configured to let the traffic pass through, then unhealthy state is reported. This is because the network function or overall service chain is Unhealthy or both are in Unhealthy state.
  - Undetermined—Down arrow in yellow. This state is reported when the health of the service chain can't be determined. This state is also reported when there's no status such as healthy or unhealthy available for the monitored service chain over a time period. You can't query or search a service chain with undetermined status.

If a service chain consists of a single PNF and PNF is outside the reachability of Cisco SD-WAN Manager, it can't be monitored. If a service chain consists of a single network function, the firewall that has VPN termination on both sides which can't be monitored, then it's reported as Undetermined.

Note
If the status of a service chain is undetermined, you can't choose the service chain to view the detailed monitoring information.

- If you had configured a service chain by enabling the monitoring field, then click a service group that is in Healthy or Unhealthy state. The primary part of the service chain monitoring window contains the following elements:

  Graphical display that plots the latency information of the service chain, VNFs, PNFs.

  The detail part of the service chain monitoring window contains:

  - Search: To filter the search results, use the Filter option in the search bar.
  - A table that lists information about all service chains, VNFs, PNFs, their health status, and types.
    - Check the service chain, VNF, PNF check boxes for the service chains, VNFs, PNFs you want to choose.
    - To change the sort order of a column, click the column title.

  The status details column indicates the monitored data path and it provides the per hop analysis.

- Click **Diagram** and view the service group with all the service chains and VNFs in the design view window.
- Click a VNF. You can view CPU, memory, and disk allocated to the VNF in a dialog box.
- Choose a service group from the **Service Groups** drop-down. The design view displays the selected service group with all the service chains and VNFs.

Step 4 Click **Network Functions**.

Here, you can view the following:

- All the virtual or physical network functions in a tabular format. Use the **Show** button, and choose to display either a VNF or PNF.

  VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, colocation user groups, CPU use, memory consumption, and other core parameters that define performance of network service. To view more information about the VNF, click a VNF name. See View Information About VNFs , on page 106 .

- PNF information is displayed in tabular format. The table includes information such as the serial number and PNF type. To view and note configuration of a specific PNF, click the desired PNF serial number. Ensure that you manually note all the configuration of the PNFs and then configure the PNF devices. For example, the following are some of the PNF configuration where you position the PNF at various locations in the service chain. See the ASR 1000 Series Aggregation Services Routers Configuration Guides and Cisco Firepower Threat Defense Configuration Guides to configure the PNFs manually.

Figure 13: PNF in the First Position with Service Chain Side Parameters

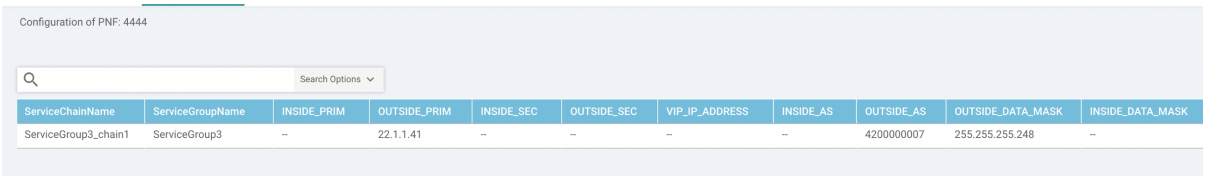


Figure 14: PNF in the First Position with Outside Neighbor Information

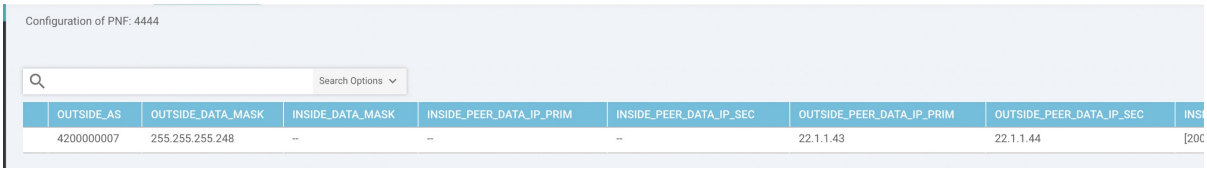


Figure 15: PNF Shared Across Two Service Chains

The ServiceGroup2_chain3 is a PNF-only service chain and therefore no configuration gets generated. The PNF is in the last position of the ServiceGroup2_chain1, so only INSIDE variables gets generated.



Figure 16: PNF Shared Across Two Service Chains with Outside Neighbor Information



Packet Capture for Cloud OnRamp Colocation Clusters

Table 43: Feature History

Feature Name	Release Information	Description
Packet Capture for Cloud OnRamp Colocation Clusters	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature lets you capture packets at either the physical network interface card (PNIC) level or the virtual network interface card (VNIC) level on a Cloud Services Platform (CSP) device of a colocation cluster. You can capture packets on one or more PNIC or VNIC on the same device or different devices with different browsers at the same time. This feature lets you gather information about the packet format, and helps in application analysis, security, and troubleshooting.

You can capture packets flowing to, through, and from a CSP device of a colocation cluster. You can capture packets at either the PNIC or the VNIC level on the CSP device.

Supported Ports for Packet Capture for Cloud OnRamp Colocation Clusters

Packet capture is supported for the following ports:

Table 44: Supported Ports for Packet Capture

Mode	VNIC Level	PNIC Level
Single Tenancy	OVS-DPDK, HA-OVS-DPDK, SR-IOV, OVS-MGMT	SR-IOV, MGMT
Multitenancy (Role-Based Access Control)	OVS-DPDK, HA-OVS-DPDK, OVS-MGMT	MGMT

Enable Packet Capture on Cisco SD-WAN Manager

Enable the packet capture feature on Cisco SD-WAN Manager before capturing packets at the PNIC or VNIC level on a CSP device of a colocation cluster:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Data Stream**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable data stream.

Capture Packets at PNIC Level

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

2. Click **Colocation Cluster**, and choose a cluster.
3. From the list of devices that is displayed, click a CSP device name.
4. In the left pane, click **Packet Capture**.
5. From the **PNIC ID** drop-down list, choose a PNIC.
6. (Optional) Click **Traffic Filter** to filter the packets that you want to capture based on the values in their IP headers.

Table 45: Packet Capture Filters

Field	Description
Source IP	Source IP address of the packet.
Source Port	Source port number of the packet.
Protocol	Protocol ID of the packet. The supported protocols are: ICMP, IGMP, TCP, UDP, ESP, AH, ICMP Version 6 (ICMPv6), IGRP, PIM, and VRRP.
Destination IP	Destination IP address of the packet.
Destination Port	Destination port number of the packet.

7. Click **Start**.

   The packet capture begins, and its progress is displayed:

   - Packet Capture in Progress: Packet capture stops after the file size reaches 20 MB, or 5 minutes after you started packet capture, or when you click **Stop**.
   - Preparing file to download: Cisco SD-WAN Manager creates a file in libpcap format (a .pcap file).
   - File ready, click to download the file: Click the download icon to download the generated file.

Capture Packets at VNIC Level

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click **Colocation Cluster**, and choose a cluster.
3. From the list of devices that is displayed, click a CSP device name.
4. Choose a VNF, and then click **Packet Capture** in the left pane.
5. Alternatively, choose **Monitor** > **Devices** > **Colocation Cluster**. Next, choose a cluster and click **Network Functions**, choose a VNF, and then click **Packet Capture** in the left pane.
6. From the **VNIC ID** drop-down list, choose a VNIC.
7. (Optional) Click **Traffic Filter** to filter the packets to capture based on values in their IP headers. For more information on these filters, see the above section.

8. Click **Start**. The packet capture begins, and displays its progress.

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Multitenancy

Table 46: Feature History

Feature Name	Release Information	Description
Colocation Multitenancy Using Role-Based Access Control	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature enables a service provider to manage multiple colocation clusters and share these clusters across tenants by using multiple colocation groups. In a multitenant setup, service providers don't need to deploy a unique colocation cluster for each tenant. Instead, the hardware resources of a colocation cluster are shared across multiple tenants. With multitenancy, service providers ensure that tenants view only their data by restricting access based on roles of individual tenant users.

Overview of Colocation Multitenancy

In Cisco Catalyst SD-WAN Cloud OnRamp for Colocation multitenancy, a service provider can manage multiple colocation clusters using Cisco SD-WAN Manager in single-tenant mode. A service provider can bring up a multitenant cluster in the same way as bringing up a cluster in a single-tenant mode. A multitenant cluster can be shared across multiple tenants. See Create and Activate Clusters.

The tenants share the hardware resources such as the Cisco Cloud Services Platform (CSP) devices and Cisco Catalyst 9500 devices of a colocation cluster. The following are the key points of this feature.

- A service provider deploys and configures the Cisco SD-WAN Control Components (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Controller) with valid certificates.
- A service provider sets up colocation clusters after onboarding the Cisco CSP devices and Cisco Catalyst 9500 switches.
- Cisco Catalyst SD-WAN operates in a single-tenant mode and Cisco SD-WAN Manager appears in a single-tenant mode.
- In a colocation multitenant deployment, a service provider ensures that tenants see only their service chains by, creating roles. A service provider creates roles for each tenant in a colocation group. These tenants are permitted to access and monitor the service chains based on their roles. However, they can’t configure their service chains or change the system-level settings. The roles ensure that tenants can access only the information that they are authorized to view.
- Each tenant traffic is segmented using VXLAN across the compute devices, and VLAN across the Cisco Catalyst switch fabric.
- A service provider can provision service chains on a specific cluster.

The following are the two scenarios of a colocation multitenant setup:

- Service provider owned Cisco Catalyst SD-WAN devices: In this scenario, the Cisco Catalyst SD-WAN devices used in a service chain belong to the corresponding service provider. The CSP devices and Catalyst 9500 switches are owned, monitored, maintained by the service provider. The virtual machine (VM) packages are owned, uploaded, and maintained by a service provider. See Monitor Colocation Cluster Devices and Cisco Catalyst SD-WAN Devices in Comanaged Multitenant Environment, on page 122.
- Comanaged Cisco Catalyst SD-WAN devices: In this scenario, the Cisco Catalyst SD-WAN devices that are used in a service chain belong to a tenant overlay network. The colocation cluster devices are owned by the service provider, whereas the Cisco Catalyst SD-WAN of a service chain are controlled by the Cisco SD-WAN Control Components (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Controller) of a tenant. The CSP devices and Catalyst 9500 switches are owned, monitored, maintained by the service provider. The VM packages are owned, uploaded, and maintained by a service provider. See Monitor Colocation Cluster Devices and Cisco Catalyst SD-WAN Devices in Comanaged Multitenant Environment, on page 122.

Roles and Functionalities in a Multitenant Environment

Multitenant environments include a service provider and multiple tenants. Each role has distinct responsibilities and associated functions.

Service Provider

A service provider owns all the hardware infrastructure and manages the clusters. The service provider also onboards tenants by creating their roles, provisions the service chains for tenants, and can view all the service chains of all the tenants.

A service provider logs in to Cisco SD-WAN Manager as the **admin** user or a user who has the write permission for the manage users' permission. A service provider can add, edit, or delete users and user groups from the Cisco SD-WAN Manager server, and is typically responsible for the following activities:

- Create and manage clusters for tenants.
- Upload prepackaged VM image packages and Cisco Enterprise NFV Infrastructure Software (NFVIS) software images on the CSP devices.
- Create custom colocation groups and role-based access control (RBAC) users.
- Create service groups and associate a colocation group to multiple service groups.
- Upgrade CSP devices and Catalyst 9500 switches.
- Monitor service chains and VMs of all the tenants.
- Start, stop, or restart operations on any of the tenant virtual network functions (VNFs).
- Administer Cisco SD-WAN Manager and record system-wide logging of Cisco Catalyst SD-WAN devices.

Tenants

Tenants can initiate operations on the VNFs for the service chains that belong to themselves, but they can't view, access, or initiate operations on VNFs for the service chains that belong to another tenant. Tenants are responsible for the following activities:

- Monitor all the service groups and the health status of the service chains that belong to themselves.
- Monitor event or alarms for VNFs that are a part of the service chains that belong to themselves.
- Initiate start, stop, or restart operations on VNFs that are a part of the service chains that belongs to themselves.
- Collaborate with the corresponding service provider for issues, if any, on cluster, service chains, or VNFs.

Recommended Specifications in a Multitenant Environment

We recommend that service providers use the following information to decide on the number of tenants, clusters, service chains per tenant, and VLANs for various colocation sizes:

Table 47: Specifications for a Multitenant Environment

Tenants	Clusters (CPUs)	Service Chains (CPUs) per Tenant	VLANs
150	2 (608)	1 (4)–Small	~300
75-150	2 (608)	2-3 (4-8)–Medium	300-450
25-50	2 (608)	4-6 (12-24)–Large	~400
300	4 (1216)	Small	~600
150-300	4 (1216)	Medium	600-900
50-100	4 (1216)	Large	~800
600	8 (2432)	Small	~1200
300-600	8 (2432)	Medium	900-1200
100-200	8 (2432)	Large	~1050
750	10 (3040)	Small	~1500
375-750	10 (3040)	Medium	600-1500
125-230	10 (3040)	Large	~1250

For example, if a service provider provisions four vCPUs per tenant for a service chain that consists of a single VM, the service provider can onboard approximately 150 tenants on two clusters with eight CSP devices. Each of these tenants or service chains requires 300 hand-off VLANs, one ingress, and one egress VLAN per service chain. .

Assumptions and Restrictions in Colocation Multitenancy

The following sections provide detailed information about the assumptions and restrictions in a colocation multitenant environment.

Assumptions

- The wiring between Cisco CSP devices and Cisco Catalyst 9500 switches is completed as per the prescriptive connections or flexible topology. To bring up multiple clusters, ensure that the wiring between the CSP devices and Catalyst 9500 switches of a cluster are in the same way as a single cluster. For more information about wiring, see Wiring Requirements.
- Each Cisco CSP device has two 1-GB management ports that are manually configured as port channels to the out of band (OOB) management switch.
- A tenant can only monitor the event or alarms from the **Monitor** window for the VNFs that are a part of the service chains that they own. The tenant-monitoring windows display the corresponding colocation group when a tenant is viewing a service chain.



Note In a comanaged multitenant setup, the service provider provisions service chains for tenants by gathering the required information from tenants. For example, a tenant provides the tenant organization name, tenant Cisco SD-WAN Validator IP address, tenant site ID, system IP address, and so on, out of band. See Create Service Chain in a Service Group, on page 75.

Restrictions

- Altering a colocation cluster from a single-tenant mode to a multitenant mode and conversely isn’t supported.
- Sharing VNF devices across multiple tenants isn't supported.
- Service providers can provision multiple service groups for a tenant. But, the same service group can’t be provisioned for multiple tenants.
- Upgrading from Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Release 20.4.1 having a single-tenant mode, to Release 20.5.1 or later having a multitenant mode isn’t supported. This restriction means you can’t upgrade from a single-tenant mode to multitenant mode.
- Multitenancy in single-root IO virtualization enabled (SR-IOV-enabled) physical network interface cards (PNICs) isn't supported; only open virtual switch (OVS) for VNF VNICs is supported. All the PNICs in the CSP devices are in OVS mode because the current SR-IOV drivers don’t support VXLAN. The VNF VNICs are connected to OVS networks, and the ability to forward traffic at the desired speed might reduce.
- Managing billing and subscription of the resources utilized by tenants isn't supported.
- In a comanaged multitenant setup, a tenant can monitor only the VNF devices that the tenant owns.

Service Provider Functionalities

Provision a New Tenant

The service provider can provision a new tenant by creating a colocation group, and then provide access to a tenant by creating an RBAC user for the user group associated with the colocation group. RBAC users can perform limited administrative duties within their own tenant environment.

Before you begin

A service provider should bring up clusters in shared mode by establishing control connections with the CSP devices and activating the cluster. The service provider can create several clusters, and each of these clusters can have between two to eight CSP devices and two Catalyst 9500 switches. The cluster-creation operation supports an option to choose if the cluster is for a multitenant or a single-tenant deployment. See Create and Activate Clusters.

Procedure

Step 1 To onboard a tenant, create a colocation group. For more information, see Create Colocation Group . This group provides access to tenants to monitor their service groups and VMs.

Step 2 Add an RBAC user and associate it with the colocation group created in Step 1. For more information, see Create an RBAC User and Associate to Colocation Group.

Note
Don't add an RBAC user if you're authenticating the user using the TACACS server instead of Cisco SD-WAN Manager. If you're authenticating a user using a TACACS server, associate the user with the colocation group created in Step 1.

Step 3 Create a service group, associate it with the colocation group, and attach the service group to a specific cluster. See Create Service Chain in a Service Group.

When a tenant requires a new service chain, use the handoff VLANs that are specific to the tenant.

Create Colocation Group

In a single-tenant Cisco SD-WAN Manager, a colocation cluster can be shared across multiple tenants by using colocation groups. The colocation groups are a mechanism to associate a service chain to a particular tenant. The RBAC users created for the tenants are called the colocation groups. These users can log in to Cisco SD-WAN Manager using their credentials to view only their tenant-specific service chains and VNF information. If the service provider chooses to use a service group for a tenant, the colocation group needs to be created prior to creating a service group so that the colocation group can be associated with the service group.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Colo Groups**.

Step 2 Click **Add Colo Group**.

Step 3 Enter a colocation group name, name of a user group with which the colocation group must be associated with, and description.

Note
The colocation group name you provide here is displayed when you create a service group for a multitenant setup.

Step 4 Click **Add**.

View Permissions of a User Group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **User Groups**.

Step 3 To view the permissions of a user group, in the**Group Name** list, and click the name of the user group that you created.

Note
The user group and their permissions are displayed. To know about the list of user group permissions in a multitenant environment, see the Manage Users topic in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

Create an RBAC User and Associate to Colocation Group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **Add User**.

Step 3 In the **Add User** dialog box, enter the full name, username, and password for the user.

Note
You can’t enter uppercase characters for usernames.

Step 4 From the **User Groups** drop-down list, add the groups that the user must belong to, by choosing one group after another, for example, a user group that you created for the colocation feature. By default, the resource group **global** is chosen.

Step 5 Click **Add**.

Cisco SD-WAN Manager now lists the user is in the **Users** table.

Note
The RBAC users who are created for tenants or colocation groups can log in to Cisco SD-WAN Manager using their credentials. These users can view their tenant-specific service chains and VNF information after the service group associated with a tenant is attached to a cluster.

Delete an RBAC User from a Colocation User Group

To delete an RBAC user, remove the RBAC user from a colocation group if the user is configured using Cisco SD-WAN Manager. If the user is authenticated using the TACACS server, disassociate the user from the user group in the TACACS server.

After an RBAC user is deleted, the user can no longer access or monitor the devices of the cluster. If an RBAC user is logged into Cisco SD-WAN Manager, deleting the user doesn't log out the RBAC user.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click an RBAC user you want to delete.

Step 3 For the RBAC user you want to delete, click **...** and choose **Delete**.

Step 4 Click **OK** to confirm the deletion of the RBAC user.

Delete Tenants

To delete a tenant, remove the service groups associated with the tenant and then remove the colocation group for the tenant.

Procedure

Step 1 Locate the list of service groups associated with the tenant that you want to delete. See View Service Groups.

Note
A tenant is a colocation group having one or more RBAC users associated to the same colocation group. In the service group configuration page, you can view the colocation group of the tenant.

Step 2 Detach the service group from the cluster for the tenant that you want to delete. See Attach or Detach a Service Group in a Cluster, on page 91.

Note
To reuse the service group for another tenant, change the colocation group associated with the service group. If you delete the service group, you need to re-create it.

Step 3 Delete the colocation group for the tenant. See the Manage a User Group topic in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

Manage Tenant Colocation Clusters

A service provider can perform the following managing tasks:

- Activate clusters: A service provider can configure devices, resource pool, system settings, and activate a cluster in the multitenant or shared mode. See Create and Activate Clusters.

- Create service groups and associate RBAC users to colocation groups: A service provider can create a colocation group, associate RBAC users to the colocation group, create a service group, associate the service group with the colocation group for the multitenant mode, and attach the service group to a specific cluster. See Create Service Chain in a Service Group.

Note A service provider must associate specific service groups for each tenant.

- Create VM packages: A service provider can create and upload the VM packages into the Cisco SD-WAN Manager repository. The same packages can be used to provision VNFs in service chains for multiple tenants.

Note When a service group is associated with a colocation group, the SR-IOV option in the VM package creation that is used for configuring the VNF, is ignored. In a multitenant mode, VNF packages support only OVS-DPDK with VXLAN.

- Monitor service chains and VNFs of tenants: A service provider can monitor all the tenant service chains and identify the service chains that are unhealthy along with the tenants associated with these service chains. The service providers can also collect logs from Cisco SD-WAN Manager or CSP devices and notify the tenants.
- Add and remove Cisco CSP devices: To manage colocation clusters, a service provider can add or remove CSP devices.

Tenant Functionalities

Manage Colocation Clusters as Tenants

All tenants must monitor the service chains and VMs associated with the service chains, and collaborate with service providers if any health issues arise with the service chains. Tenants can only monitor those events or alarms for VNFs that are a part of the service chains that belongs to the tenant.

Tenants don't have any administrative privileges and can only see the service chains that service providers create. The tenant-monitoring windows display the corresponding colocation group when a tenant is viewing service chains. Tenants can perform the following tasks:

1. Log in to Cisco SD-WAN Manager as a tenant by entering the RBAC username and password.
2. View and monitor the health of the tenant service chains along with the health of the VNFs. To know more about the different service chain health statuses, see Monitor Cloud OnRamp Colocation Clusters, on page 108.

   In the **Monitor. Network** window, click **Diagram** for a service chain to view all the tenant service groups along with the service chains and VNFs in the design view.
3. View the VNF health of a tenant:
   a. In the Monitor window, click **Network Functions**.
   b. Click a VNF name from the **Virtual NF** table.

In the left pane, click **CPU Utilization**, **Memory Utilization**, and **Disk Utilization** to monitor the resources utilization of a VNF.

You can also view the VM-specific alarms and events from the left pane.

4. Start, stop, or reboot a VNF:
   a. In the Monitor window, click a VNF name from the **Virtual NF** table.
   b. For the clicked VNF name, click **...** and choose one of the following operations:
      - **Start**
      - **Stop**
      - **Restart**

Monitor Colocation Cluster Devices and Cisco Catalyst SD-WAN Devices in Comanaged Multitenant Environment

Before you begin

- When creating a service chain using a service provider Cisco SD-WAN Manager, the service provider should ensure that the correct UUID, and device OTP for the Cisco Catalyst SD-WAN VM in a service chain are entered. The service provider has no access to the tenant overlay, and therefore, a tenant should provide this information.
- When a service provider detaches a service group from a colocation cluster, the service provider should notify the tenant that the corresponding VM devices must be decommissioned using the tenant Cisco SD-WAN Manager.
- If a service provider needs to reattach a service group to a colocation cluster, a new OTP of the Cisco Catalyst SD-WAN VM should be entered. This OTP is provided by the tenant. The service group in the service provider Cisco SD-WAN Manager should be edited to save the new OTP of the Cisco SD-WAN VM.

Procedure

Step 1 Associate the tenant Cisco Catalyst SD-WAN devices with the service provider service group when creating a service chain. See Create Service Chain in a Service Group.

Step 2 Monitor the VNFs from the service provider Cisco SD-WAN Manager. See Monitor Cloud OnRamp Colocation Clusters.

Step 3 Monitor the information about the Cisco Catalyst SD-WAN devices of the VNFs from the tenant Cisco SD-WAN Manager.

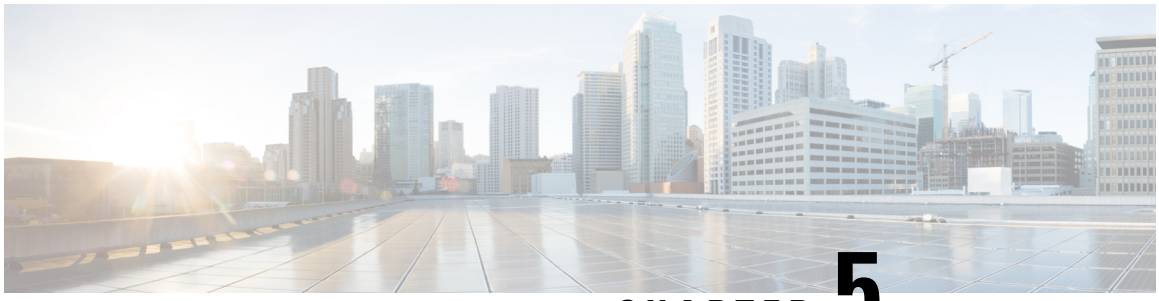
Note
The service provider can't view information about the Cisco Catalyst SD-WAN devices of the VNFs from the service provider **Configuration** > **Devices** window under **WAN Edge List**, because these devices are controlled by the tenant.



PART I

Cloud OnRamp for SaaS

- Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later, on page 125
- Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x, on page 137
- Application Lists, on page 201
- Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, on page 207



CHAPTER 5

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later

Note For information about template-based configuration of Cloud OnRamp for SaaS in earlier releases, see Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x, on page 137.

- Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later, on page 126
- Information About Cloud OnRamp for SaaS, on page 126
- User-defined probe endpoints for applications, on page 127
- Cloud OnRamp for SaaS capable applications, on page 127
- Prerequisites for Cloud OnRamp for SaaS, on page 127
- Restrictions for Cloud OnRamp for SaaS, General, on page 128
- Restrictions for Service VPN Gateway Mode, on page 128
- Configure Cloud OnRamp for SaaS Using a Workflow, on page 129
- Add SaaS Applications Using Policy Groups, on page 129
- Deploy SaaS Applications Using Policy Groups, on page 131
- Add a user-defined endpoint to applications, on page 131
- Monitor Cloud OnRamp for SaaS, on page 133
- Migrate Older Cloud OnRamp for SaaS Path Selection, on page 134

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later

Table 48: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for SaaS Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Control Components Release 20.15.1	Cisco SD-WAN Manager provides a fully-guided workflow for selecting specific applications to enable Cloud OnRamp for SaaS. Cloud OnRamp for SaaS identifies the best paths for handling traffic for each of these applications.
Cloud OnRamp for SaaS for user-defined SaaS application lists	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Cisco SD-WAN Manager supports adding, editing, and deleting user-defined probe endpoints for applications listed in the application catalog. Applications with endpoint details are eligible for: • cloud monitoring, and • steering through best path. You can also create an application list with applications having a common probe endpoint and enable Cloud OnRamp for SaaS for that application list.

Information About Cloud OnRamp for SaaS

Cloud OnRamp for SaaS can determine the best network path for each type SaaS application, also called cloud application, traffic. Select specific SaaS applications and Cloud OnRamp for SaaS identifies the best traffic paths for each of the SaaS applications.

Benefits

An organization with multiple branch offices can use Cloud OnRamp for SaaS to ensure that SaaS application traffic at each office uses the most efficient path. Using the most efficient path ensures that the employees at different locations experience consistent and high-quality access to cloud services such as Microsoft Office 365, Salesforce, or Google Workspace.

User-defined probe endpoints for applications

User-defined probe endpoint support is an enhancement that:

- enables adding probe endpoint details directly to applications in the Application Catalog,
- enables any application in the Application Catalog having probe endpoint details to be considered capable of cloud monitoring and/or steering through the best path using Cloud SLA action,
- provides a distinct view of user-defined cloud application lists and all application lists in the guided workflow, and
- simplifies the creation and deployment of application lists with applications having a common user-defined endpoint through a guided workflow.

Cloud OnRamp for SaaS capable applications

An application in Application Catalog that includes endpoint details is capable of supporting:

- Cloud Monitoring: Enabling detailed visibility and monitoring of these applications, and
- Cloud SLA: Ensuring that applications are steered through the best path computed with cloud monitoring.

A Cloud OnRamp for SaaS capable application list includes the following types of application lists:

- Default cloud application lists: 14 predefined application groups with predefined endpoints.
- User-defined cloud application lists: Application lists with applications that have common user-defined endpoints.

To use Cloud OnRamp SaaS capable application lists in policy groups, see the following procedures:

- configure using the workflow: Configure Cloud OnRamp for SaaS Using a Workflow, on page 129
- configure using the procedure: Add SaaS Applications Using Policy Groups, on page 129, and
- deploy using the procedure: Deploy SaaS Applications Using Policy Groups, on page 131.

Prerequisites for Cloud OnRamp for SaaS

- To enable Cloud OnRamp for SaaS for Webex and Microsoft Office 365 applications, ensure that Cisco SD-AVC is enabled (**Administration** > **Cluster Management**).

  Enable Cisco SD-AVC and cloud services.

  For Cisco Catalyst SD-WAN Manager Release 20.16.1 and earlier, enable cloud services in Cisco Catalyst SD-WAN. This also enables the Cisco SD-AVC Cloud Connector. For information on how to enable SD-AVC on SD-WAN Manager, see Enable SD-AVC for Cisco SD-WAN devices.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-AVC is enabled by default in SD-WAN Manager.

- To enable Cloud OnRamp for SaaS for Webex, verify that SD-WAN Manager can reach this domain:

  https://info.net-int.infra.webex.com/v1/prefixes/regions

Restrictions for Cloud OnRamp for SaaS, General

Maximum supported applications

A Cloud OnRamp for SaaS capable application list supports maximum eight applications with common endpoint. A device supports maximum of eight user-defined application lists.

Support for SIG tunnels only

If you choose Secure Internet Gateway for Internet Offload Traffic for Cloud OnRamp for SaaS capable applications, it is supported only with the SIG tunnels.

Operation with UTD

When using Cloud OnRamp for SaaS together with Cisco United Threat Defense (UTD), DNS responses may be dropped in any of these conditions:

- Cloud OnRamp for SaaS over Cisco Secure Internet Gateway (SIG) tunnels
- Cloud OnRamp for SaaS over Cisco Secure Service Edge (SSE) tunnels

  (relevant from SD-WAN Control Components 26.1.1.1)
- Cloud OnRamp for SaaS over a service VPN gateway

We recommend configuring a firewall rule, with an allow action, to skip UTD inspection for DNS requests and responses.

DNS traffic handling

As a general policy restriction not specific to Cloud OnRamp for SaaS, data policy does not support both of these conditions together:

- Data policy redirecting DNS traffic to Umbrella
- Secure Internet Gateway (SIG) configured

This restriction is relevant when considering the DNS resolver prioritization for application traffic in the context of Cloud OnRamp for SaaS.

Restrictions for Service VPN Gateway Mode

When you change the VPN settings of the service-VPN DIA interface, and Cloud OnRamp for SaaS is running in service-VPN Gateway mode, Cloud OnRamp for SaaS fails to work with the new service-VPN settings. The system continues to display stale data from the previous service-VPN setting for up to 10 minutes following the change and there is no data for the new service-VPN settings.

(Task)To prevent the issue, perform the following steps:

1. Detach the site from Cloud OnRamp for SaaS sites.
2. Update the VPN settings for the desired DIA interface on the Interface Configuration page.
3. Re-attach the site to Cloud OnRamp for SaaS as a service-VPN Gateway site.

Configure Cloud OnRamp for SaaS Using a Workflow

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library** > **Cloud OnRamp for SaaS**.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the application list displays separate lists for default cloud application lists and user-defined cloud application lists. Additionally, there is a tab that displays all available applications.

Step 2 Follow the on-screen instructions to complete the workflow.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you have the following options:

- In the **Select application lists** step of the workflow, you can use **+ Add application list** for the following:
  - Create user-defined list with applications having a common probe endpoint. For more information about defining a probe endpoint, see Add a user-defined endpoint to applications, on page 131.
  - Create custom applications with probe endpoints and associate the newly created applications in a new user-defined cloud application list.

    To create an inline custom application list with applications having a probe endpoint, follow these steps:

    a. Click on the **Applications with probe endpoint** dropdown.

    b. Click **+Add Custom Application** and fill the required fields.

    For more information about configuring a custom application with endpoint, see Configure Custom Applications.

- In the **Select Policy** step of the workflow, you can view the devices associated with the policy group and review their update status.

Step 3 When the workflow is complete, you'll be prompted with a success screen to add policies to a policy group or associate devices with the policy groups or deploy the policy groups to the devices.

Add SaaS Applications Using Policy Groups

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.

2. Create a new **Application Priority & SLA** or edit an existing Application Priority & SLA.

   For more information, see Application Priority & SLA.

Note Use either **Secure Internet Gateway** or **Direct Internet Access** to choose an Cloud OnRamp for SaaS capable appication list.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the following scenarios occur depending on whether the application list is Cloud OnRamp for SaaS capable or not Cloud OnRamp for SaaS capable.

- If the application list is Cloud OnRamp for SaaS capable, a cloud SaaS sequence is generated for that application list.
- If the application list is not Cloud OnRamp for SaaS capable, the application list has NAT DIA or SIG configuration.

3. If you are an advanced user, switch to the **Advanced Layout** and configure Cloud OnRamp for SaaS.
   For more information, see Advanced Layout.

Note

- Choose Cloud OnRamp for SaaS applications from the **Application (Lists)** drop-down list in the **Match** field. For more information on match conditions, see Configure Traffic Rules.

  Note When deploying Cloud onRamp for SaaS or DIA app-based steering, exclude internal and private destination prefixes from optimization and local-exit policy.

- Choose **Cloud Monitoring** and **Cloud SLA** as **Action** conditions. For more information on action conditions, see Configure Traffic Rules.

Note In the **Advanced Layout**, if you choose an application list that is Cloud OnRamp for SaaS capable and add cloud SaaS actions to the sequence, Cisco SD-WAN Manager generates corresponding App-route policy sequence and Cloud OnRamp for SaaS probe configuration for Cisco IOS XE Catalyst SD-WAN edge device.

If you choose an application list that is not Cloud OnRamp for SaaS capable and add cloud SaaS actions, a warning message appears when you save the configuration. The message informs you that the application list contains applications that are not Cloud OnRamp for SaaS capable. This implies that some applications in the application list have no endpoints or have different endpoints.

The Cloud OnRamp for SaaS probe configuration for this application list is not generated in the Cisco IOS XE Catalyst SD-WAN edge device.

Deploy SaaS Applications Using Policy Groups

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**. The application priority you just created appears here in the list.
2. In the **Policy Group** tab, choose a policy group to deploy. Choose the respective application priority from the drop-down list and click **Deploy**.

   For information about deploying policy groups, see Deploy Policy Groups Workflow.

   - When you've included Cloud OnRamp for SaaS applications in the policy group, the deploy workflow provides options to choose device variables such as **Site Type**, **TLOC**. Cisco SD-WAN Manager populates these fields with default values.
   - Enable **Secure Internet Gateway (SIG) Interface** if you want to secure your internet gateway.
   - Select **Enable Load Balancing** to balance the traffic using cloud SaaS probe.
   - Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, choose **None** to remove the probe configuration from the applications for a selected site. This option is useful when there are multiple sites associated to a policy group. It allows you to remove the Cloud OnRamp for SaaS capability on specific sites by removing the Cisco SD-WAN Edge probe configuration.

Add a user-defined endpoint to applications

You can add or remove endpoint details for any application in the application catalog using the following procedure.

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

- Review the prerequisites and restrictions sections for SaaS application lists.

Procedure

	If..	Then..
Step 1	You want to add endpoint details for an existing application, which also includes custom applications.	From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Applications**.
	You want to create a custom application with endpoint details.	From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Custom Application**.

Step 2 Follow one of the following procedures to add probe endpoint for an application or multiple applications:

a) To add or edit endpoint details for an existing application, click the ellipsis icon (**...**) next to the application under **Action** and click **Edit**.

Note
If you edit an application list or applications in an application list, you must save the Application Priority and SLA policy again.

b) (Optional) To create a custom application with endpoint details, click **Custom Application**.

To create a custom application with endpoint details, click **Custom Application** and follow the steps mentioned here. After defining the custom application, you can choose to add the endpoint details for it. For more information, see Configure Custom Applications.

Note
For custom applications, to prevent packet loss, do one of the following:

- Add a valid traffic class and business relevance while entering endpoint details on the Application Catalog page. This is the most preferable option.
- Switch to Advanced layout and add data policy sequences.
- Change the policy's default action to "accept."

This action prevents packets from being dropped if you choose the simple layout in Application Policy and SLA with the default action set to "drop".

Alternately, do the following:

a) Choose an application or multiple applications from the application list to add a user-defined endpoint. You can also filter specific applications using the **Search** field.
b) Click **Define Probe Endpoint**.

The applications that you choose are added to the **Selected Application(s)** area, which shows each application.

Step 3 In the **SaaS probe endpoint type** area, choose an endpoint type from the following options:

- **IP Address**: Enter an IP address. Cloud OnRamp for SaaS probes the server using port 80.
- **FQDN**: Enter a fully qualified domain name.
- **URL**: Enter a URL using HTTP or HTTPS. Cloud OnRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.

Step 4 In **SaaS probe endpoint value** field, enter an endpoint value, based on the endpoint type that you choose.

Example:

192.168.0.1, https://www.example.com, www.google.com

Step 5 Click **Save**.

(Optional) After adding endpoint details, you can also remove them. To remove the endpoint details of an application, click the ellipsis icon (**...**) next to the application under **Action** and click **Edit**. Navigate to the SaaS probe endpoint value area and remove the value field. Ensure you save the changes.

Monitor Cloud OnRamp for SaaS

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

The **Application Snapshots** section displays information such as the number of active sites, and device health.

Step 2 To view the applications that Cloud OnRamp for SaaS is monitoring, click the **Sites** tab.

Table 49: Site Information

Field	Description
Site Name	Site name.
Sites List	Site list that the site is associated with.
Device Name	Device name.
Monitored Applications	Monitored applications.
Site Role	Site role.

The view options include showing only active or inactive sites.

Step 3 To view the details of a site, click site name.

Table 50: Site Details

Field	Description
Application	Application associated with the site.
vQoE Status	The vQoE status is a monitoring indicator for the currently selected best path for the application, and not a failover threshold. It does not directly influence the Cloud OnRamp for SaaS determination of best path. A green circle with a tick indicates that vQoE is good, the status with ! indicates that the vQoE needs some attention, and red X indicates that the vQoE is poor.
vQoE Score	The vQoE score is a monitoring indicator for the currently selected best path for the application, and not a failover threshold. It does not directly influence the Cloud OnRamp for SaaS determination of best path. Select the score to view detailed charts about the score.

Field	Description
DIA (Direct Internet Access) Status	• gateway: Cloud OnRamp for SaaS is routing the application through a gateway site for internet access. • local: Cloud OnRamp for SaaS is routing the application through a local DIA link for internet access. • none: Cloud OnRamp for SaaS does not have a best path for the application.
Selected Interfaces	List of interfaces associated with the application.
Activated Gateways	For a site that connects to the internet through a gateway site, this indicates the IP address of the gateway site.
Local color	For a site that connects to the internet through a gateway site, this is the local color identifier of the tunnel used to connect to the gateway site.
Remote color	For a site that connects to the internet through a gateway site, this is the remote (gateway site) color identifier of the tunnel used to connect to the gateway site.
Application Usage	You can apply filters to view the specific types of data.

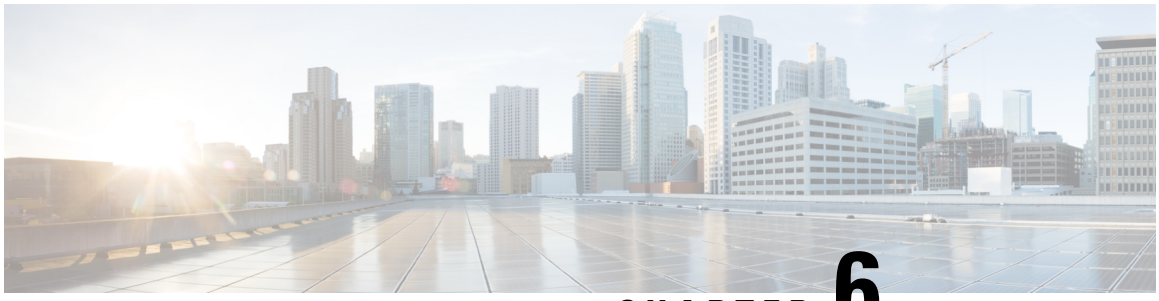
Step 4 To view configuration details, such as the configuration source, policy, number of devices, and so on, click the **Configuration** tab.

Migrate Older Cloud OnRamp for SaaS Path Selection

If you have enabled Cloud OnRamp for SaaS best path selection using the **Application and Policy** page before Cisco Catalyst SD-WAN Manager Release 20.15.1, you must perform the following procedure to configure these applications using the Cloud OnRamp for SaaS workflow:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS** > **Configuration**.
2. The first entry in the configuration tab shows the old app route policies in your Cisco SD-WAN Manager named as **Template Config**.
3. In the **Actions** column, click **...** and choose **Gateways**.
4. Choose the respective Site id and click **Detach Gateways**.
5. Follow the same instructions to detach **Applications and Policy**, **Client Sites**, **DIA Sites**, and **Custom Application Lists**.
6. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
7. On the **Device Templates** page, click **...** adjacent to the device and choose the **Detach Devices** option next to the respective device template to detach the device.
8. Configure the device using Configuration Groups. For more information, see Configuration Groups.

9. Follow the instructions to access the Cloud OnRamp for SaaS workflow and deploy using policy groups. For more information, see Deploy policy group.



CHAPTER 6

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x

- Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x, on page 137
- Information About Cloud OnRamp for SaaS, on page 140
- Supported Devices for Cloud onRamp for SaaS, on page 152
- Prerequisites for Cloud OnRamp for SaaS, on page 153
- Restrictions for Cloud onRamp for SaaS, on page 156
- Use Cases for Cloud onRamp for SaaS, on page 158
- Configure Cloud onRamp for SaaS, on page 160
- Verify Cloud onRamp for SaaS, on page 179
- Monitor Cloud onRamp for SaaS, on page 182
- Cloud onRamp for SaaS Over SIG Tunnels, on page 187
- Troubleshooting Cloud OnRamp for SaaS, on page 196

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x

Table 51: Feature History

Feature Name	Release Information	Description
Support for Specifying Office 365 Traffic Categories for Cloud OnRamp for SaaS on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature updates the existing Cloud OnRamp for SaaS configuration workflow for Cisco IOS XE Catalyst SD-WAN devices. The feature allows you to limit the use of best path selection to some or all Office 365 traffic, according to the Office 365 traffic categories defined by Microsoft.

Feature Name	Release Information	Description
Application Feedback Metrics for Office 365 Best Path Selection on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature adds new metrics as inputs to the best-path selection algorithm for Office 365 traffic. The new inputs include best-path metrics from Microsoft Cloud Services. The feature also provides a new page for viewing detailed logs of the input data used by the best path algorithm.
Load Balancing Across Multiple Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds the ability to balance traffic for cloud applications across multiple DIA interfaces.
Support for Cloud OnRamp for SaaS Probing through VPN 0 Interfaces at Gateway Sites	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Cloud OnRamp for SaaS tests the performance of (probes) routing paths to find the best routing path for specific cloud application traffic. Using the best routing path for the traffic of a cloud application optimizes the performance of the application. This feature enables Cloud OnRamp for SaaS to probe through VPN 0 interfaces at gateway sites as part of determining the best path to use for the traffic of specified cloud applications. This extends the best path probing to include more of the available interfaces connected to the internet. Using this feature, Cloud OnRamp for SaaS can probe interfaces at a gateway site, whether they use service VPNs (VPN 1, VPN 2, and so on) or the transport VPN (VPN 0). This is helpful when a branch site connects to the internet, exclusively or in part, through a gateway site that uses a VPN 0 interface to connect to the internet.
Cloud OnRamp for SaaS Support for Webex	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature adds Webex to the list of cloud applications supported by Cloud OnRamp for SaaS. Cloud OnRamp for SaaS can determine the best network path to Webex cloud servers. Cisco SD-WAN Manager periodically downloads a list of Webex servers organized by geographic region. Cloud OnRamp for SaaS uses this server list to help calculate the best network path for Webex traffic in different regions.
Support for Using Microsoft Telemetry Metrics for Microsoft 365 SharePoint and Teams Traffic.	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1	This feature adds support for using Microsoft telemetry metrics for Microsoft 365 SharePoint and Teams. Cloud OnRamp for SaaS uses the metrics data when determining the best path for Office 365 traffic.

Feature Name	Release Information	Description
View Details of Microsoft Telemetry and View Application Server Information for Office 365 Traffic	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature adds better visibility into how Cloud OnRamp for SaaS determines the best path for Microsoft Office 365 traffic, if you have opted to use Microsoft telemetry. One enhancement is a chart that shows how Microsoft rates the connection quality of different interfaces, specifically for different types (called service areas) of Office 365 traffic. This is helpful for troubleshooting Office 365 performance issues. Another addition is the **SD-AVC Cloud Connector** page, which shows a list of Microsoft URL and IP endpoints and categories that Cisco Catalyst SD-WAN receives from Microsoft Cloud.
Configure the Traffic Category and Service Area for Specific Policies	Cisco vManage Release 20.9.1 Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	You can edit AAR policies individually to change the specified Microsoft 365 traffic category and service area for specific AAR policies.
Enable Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites	Cisco vManage Release 20.9.1 Cisco IOS XE Release 17.2.1	This feature allows you to selectively delete AAR policy sequences to exclude Cloud OnRamp for SaaS operation on specific applications at specific sites.
Improved Visibility for Microsoft 365 Traffic	Cisco vManage Release 20.9.1 Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This feature provides improved visibility to allow you to monitor the details of Microsoft 365 traffic processed by Cloud OnRamp for SaaS.
Option to Include or Exclude Microsoft Telemetry Data from Best Path Decision for Microsoft 365 Traffic	Cisco vManage Release 20.9.1	This feature allows you to choose whether Cloud OnRamp for SaaS should factor in the Microsoft telemetry data in the best path decision. If you disable this option, you can still view the Microsoft telemetry data in the Cisco SD-WAN Analytics dashboard, but it does not affect the best path decision.

Feature Name	Release Information	Description
Improved Visibility and Control of Webex Traffic	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature introduces several improvements to the visibility and control of Webex traffic, including the following: • Using Cisco SD-AVC to manage deep packet inspection (DPI) of Webex traffic • Receiving server-side Webex metrics to provide detailed information about Webex traffic performance • Adding only a single sequence to application-aware routing (AAR) policies to enable Cloud OnRamp for SaaS for Webex traffic
Add Cloud OnRamp for SaaS Support for Loopback, Dialer, and Subinterfaces	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	This feature extends the Cloud OnRamp for SaaS support to SD-WAN supported WAN interfaces that includes loopback, dialer, and subinterfaces. It also adds support for TLOC-extension and SIG on loopback, dialer, and subinterfaces.
Option to Exclude Data Prefixes from Cloud OnRamp for SaaS Optimization	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	You can define a list of IP prefixes to exclude from Cloud OnRamp for SaaS optimization. This is useful when SaaS applications are hosted on-premises or in a private cloud.
Enable Faster Failover by Associating a DIA Tracker with Cloud OnRamp for SaaS	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	To enable faster failover from a failed route, you can associate a tracker to a DIA or gateway site. The tracker detects internet connectivity failure on an interface faster than Cloud OnRamp for SaaS probing.

Information About Cloud OnRamp for SaaS

Many organizations rely on software-as-a-service (SaaS) applications for business-critical functions. These cloud-based services include Amazon AWS, Box, Dropbox, Google Apps, Office 365, and many others. As cloud-based services, these SaaS applications must communicate with their own remote servers, which are available through internet connections.

At remote sites, SaaS applications may pose these special challenges:

- **Performance**: If remote sites, such as branch offices, route SaaS traffic through a centralized location, such as a data center, performance degrades, with latency that affects the user experience.

- **Inability to optimize routing**: Network administrators may not have any visibility into the performance of these SaaS applications, or any ability to change the routing of the SaaS traffic to more efficient paths.

Cloud OnRamp for SaaS (formerly called CloudExpress service) addresses these challenges. It enables you to select specific SaaS applications and interfaces, and to let Cisco Catalyst SD-WAN determine the best performing path for each SaaS application, using the specified interfaces. For example, you can enable:

- routing through a direct internet access (DIA) connection at a branch site, if available
- routing through a gateway location, such as a regional data center

Ensuring the best path for cloud traffic is critical. SD-WAN monitors each available path for each SaaS application continually, so if a problem occurs in one path, it can adjust dynamically and move SaaS traffic to a better path.

Common Scenarios for Using Cloud onRamp for SaaS

For an organization using SD-WAN, a branch site typically routes SaaS application traffic by default over SD-WAN overlay links to a data center. From the data center, the SaaS traffic reaches the SaaS server.

For example, in a large organization with a central data center and branch sites, employees might use Office 365 at a branch site. By default, the Office 365 traffic at a branch site would be routed over SD-WAN overlay links to a centralized data center, and from there to the Office 365 cloud server.

Scenario 1: If the branch site has a direct internet access (DIA) connection, you may choose to improve performance by routing the SaaS traffic through that direct route, bypassing the data center.

Scenario 2: If the branch site connects to a gateway site that has DIA links, you may choose to enable SaaS traffic to use the DIA of the gateway site.

Scenario 3: Hybrid method.

Scenario 1: Cloud Access through Direct Internet Access Links

In this scenario, a branch site has one or more direct internet access (DIA) links, as shown in the illustration below.

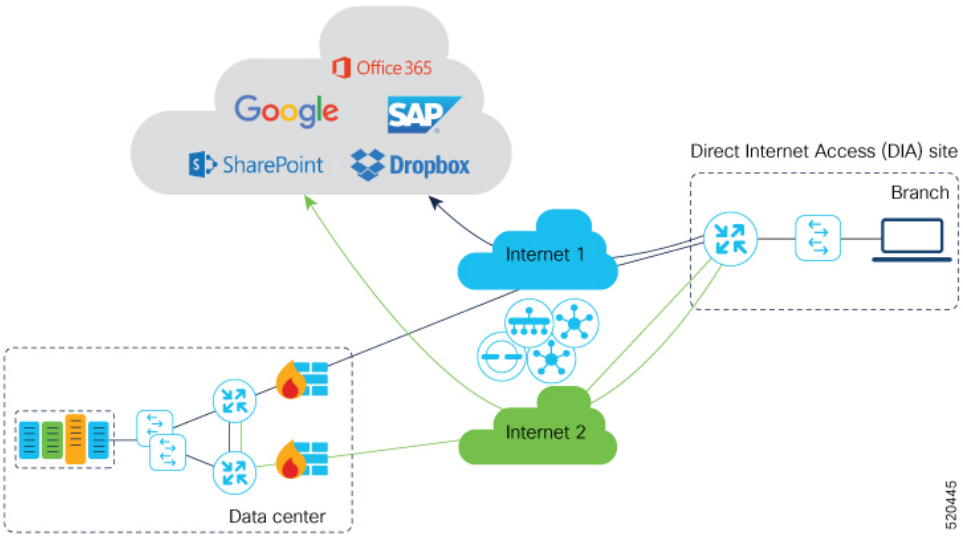
- Cloud OnRamp determining best path

  Cloud OnRamp for SaaS selects the best connection for each SaaS application through the local DIA links that are configured and available. For Cloud OnRamp for SaaS, a DIA link is considered unavailable in various conditions—for example, loss of more than 90% of probe packets.

- Cloud OnRamp not determining best path

  If Cloud OnRamp for SaaS determines that no local DIA paths are available for an application, the traffic follows the path determined by other routing features on the site.

Note that the best connection may differ for different SaaS applications. For example, Office365 traffic may be faster through one link, and Dropbox traffic may be faster through a different link.



Overview of the configuration tasks:

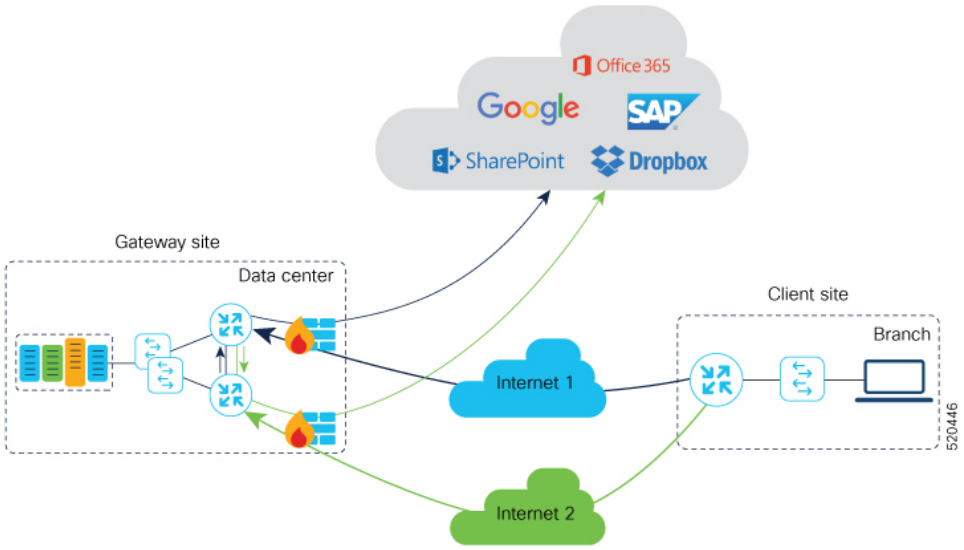
Enable Cloud OnRamp for SaaS, select the applications for which Cloud OnRamp for SaaS will find the best-performing path, choose the policy to steer traffic through the best-performing path, and associate the policy with DIA sites.

1. Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices, on page 160
2. Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 161
3. Configure Direct Internet Access (DIA) Sites, on page 170

Scenario 2: Cloud Access through a Gateway Site

In this scenario, a branch site has one or more direct connections to a gateway site, and the gateway site has links to the internet.

Using Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN can select the best connection for each SaaS application through the gateway site. If the branch site connects to more than one gateway site, SD-WAN ensures that SaaS traffic uses the best path for each SaaS application, even through different gateway sites.



Overview of the configuration tasks:

Enable Cloud OnRamp for SaaS, select the applications for which Cloud OnRamp for SaaS will find the best-performing path, choose the policy to steer traffic through the best-performing path, and associate the policy with client sites and gateway sites.

1. Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices, on page 160
2. Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 161
3. Configure Client Sites, on page 165
4. Edit Interfaces on Gateway Sites, on page 168

Scenario 3: Hybrid Approach

In this scenario, a branch site has both direct internet access (DIA) links, and links to a gateway site, which also has links to the internet.

Using Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN can select the best connection for each SaaS application, either through DIA links or through the gateway site.

Overview of the configuration tasks:

Enable Cloud OnRamp for SaaS, select the applications for which Cloud OnRamp for SaaS will find the best-performing path, choose the policy to steer traffic through the best-performing path, and associate the policy with DIA sites and gateway sites.

1. Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices, on page 160
2. Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 161
3. Configure Direct Internet Access (DIA) Sites, on page 170
4. Edit Interfaces on Gateway Sites, on page 168

Specify Office 365 Traffic Category

When enabling Cloud onRamp for SaaS to manage Office 365 traffic, you can limit Cloud onRamp for SaaS path selection to apply to some or all Office 365 traffic, with the following options:

- **Optimize** traffic
- **Optimize** and **Allow** traffic
- All Office 365 traffic

These options correspond to the three categories of Office 365 traffic that Microsoft defines as follows:

- **Optimize**: Traffic most sensitive to network performance, latency, and availability.
- **Allow**: Traffic less sensitive to network performance, latency, and availability.
- **Default**: Traffic not sensitive to network performance.

Specifying traffic by Office 365 category requires enabling the Cisco SD-AVC Cloud Connector component in **Administration** > **Settings**.

Best path determination

Cloud OnRamp for SaaS selects the best path for each application using an algorithm that takes input from the sources shown in the table. The algorithm chooses among the configured and available Cloud OnRamp internet egress options for an application, such as local DIA egress or gateway site internet egress. The vQoE status and vQoE score displayed on the monitoring page are monitoring indicators and are not failover thresholds. They do not directly influence the Cloud OnRamp for SaaS determination of best path.

	Input	All Cloud Application Traffic	Office 365 Traffic
1	Cloud OnRamp for SaaS metrics based on path probing	Yes	Yes
2	Application response time (ART) metrics	No	Yes (if enabled)
3	Microsoft telemetry metrics	No	Yes (if enabled)

For Office 365 traffic, you can view a log of the metrics that factor into the best-path determination. The metrics appear in a Cisco SD-WAN Analytics page specifically designed to display only this information, and available directly from Cisco SD-WAN Manager.

Load Balancing Across Multiple Interfaces

Cloud onRamp for SaaS can determine the best network path for each type of cloud traffic. However, if multiple direct internet access (DIA) interfaces on a WAN edge device at a branch site provide acceptable performance for a cloud application, Cloud onRamp for SaaS can employ load balancing across up to three interfaces to further improve performance.

When you enable load balancing across multiple interfaces of a WAN edge device, load balancing is enabled for all cloud applications that are managed by Cloud onRamp for SaaS. After determining the best path

interface for a cloud application, Cloud onRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the following must be true:

- The packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than a configured value (%). You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface.
- The latency value of the interface cannot vary from the latency value of the best path interface by more than a configured value (milliseconds). You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface.

If required, you can select an option to ensure that all traffic from a single host uses a single interface – for example, to ensure that DNS and application traffic use the same path.

Information About Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

A branch site may connect to the internet through one or more direct internet access (DIA) interfaces at the branch site itself, or through a gateway site, which might use a service VPN or VPN 0 to connect to the internet.

In addition to probing the DIA interfaces at a branch site, Cloud OnRamp for SaaS can probe interfaces at a gateway site, whether they use service VPNs (VPN 1, VPN 2, …) or the transport VPN (VPN 0), when determining the best path to use for the traffic of specified cloud applications. This is helpful when the branch site connects to the internet through a gateway site.

When configuring Cloud OnRamp for SaaS to use the gateway site, specify whether the gateway site uses service VPNs or VPN 0 to connect to the internet, as shown in the following illustrations.

Figure 17: Branch Site Connects to a Gateway Site That Uses Service VPNs to Connect to the Internet

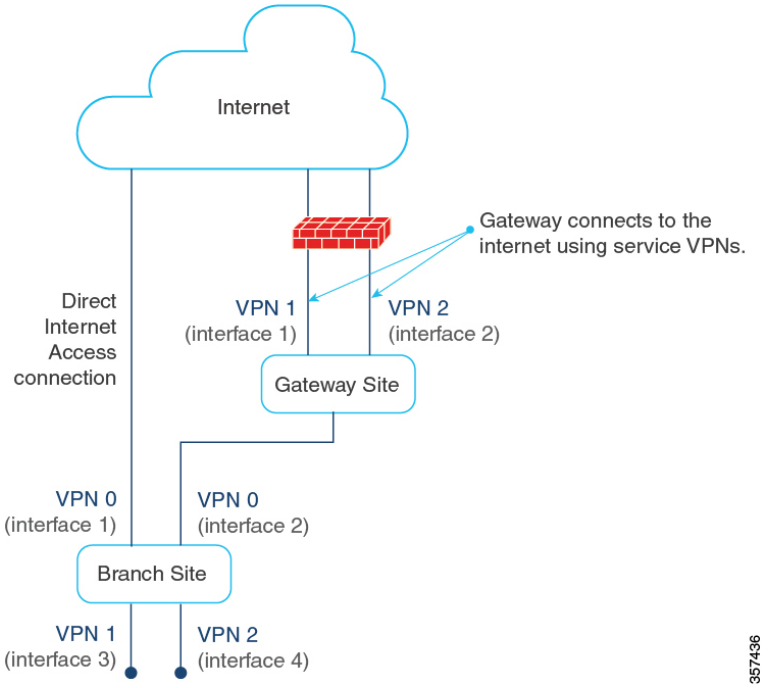
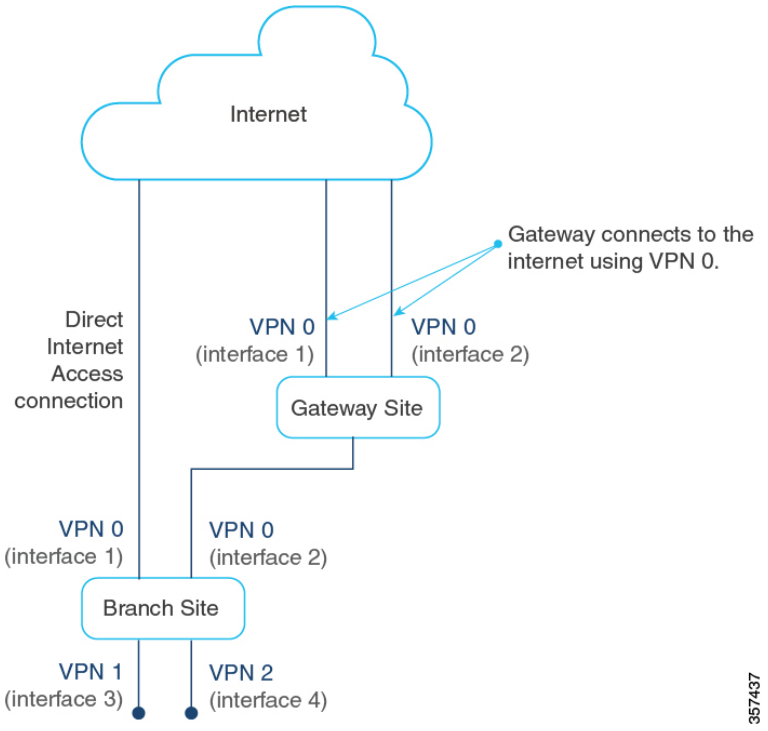


Figure 18: Branch Site Connects to a Gateway Site That Uses VPN 0 to Connect to the Internet



Information About Cloud OnRamp for SaaS Support for Webex

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

When you enable Cloud OnRamp for SaaS best path determination for an application, Cisco SD-WAN Manager updates match conditions in the application-aware policy in the active centralized policy to support Cloud OnRamp for SaaS functionality for the application. For most applications, the match conditions do not require any later update.

For Webex, Cloud OnRamp for SaaS uses a more complex method than for most other applications. Cloud OnRamp for SaaS maintains a list of worldwide Webex servers. When you enable Cloud OnRamp for SaaS best path determination for Webex, Cloud OnRamp for SaaS determines the best path for each Webex server worldwide. It adds match conditions in the application-aware policy to address each of the regional Webex servers. This provides the Webex application with the best path to any Webex server worldwide that it may need to connect to.

In the Cisco SD-WAN Release 20.9.1 Cloud OnRamp for SaaS Support for Webex, when a Webex API response contains `provider_reserved`, it will result in a `sync push failed` response.

When this issue occurs in a customer deployment:

- New Deployments: Customers need to upgrade to the latest 20.9 version or 20.12+.
- Existing Deployments: Customers need to upgrade to the latest 20.9 version or 20.12+. If an upgrade is not an option, please contact TAC.

Table 52: Best Path Determination Method for Webex, Compared with the Method for Other Applications

Application	Cloud OnRamp for SaaS Method
Most cloud applications	Cloud OnRamp for SaaS determines the best path to the most relevant server for the cloud application, as determined by the DNS response, using the DNS server configured for the device.
Webex	Cloud OnRamp for SaaS maintains a list of worldwide Webex servers, and determines the best path for all available Webex servers.

Maintaining an Up-to-Date List of Webex Servers

To maintain an up-to-date list of Webex servers, Cisco SD-WAN Manager periodically retrieves the latest server information and determines whether there are any changes to the information. If Cisco SD-WAN Manager detects that there are changes to the Webex server information, it displays notifications on the Cloud OnRamp for SaaS dashboard, prompting you to synchronize the Webex server information. The notifications are shown in a dialog box that appears on the Cloud OnRamp for SaaS dashboard page, and in a message in the Webex application pane that appears on the dashboard.

Classifying Traffic with SD-AVC

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cloud OnRamp for SaaS uses Cisco SD-AVC to manage deep packet inspection (DPI) of Webex traffic, enabling first-packet classification of the traffic. This requires enabling SD-AVC in **Administration** > **Settings**.

Classifying Webex traffic flows from the first packet enables Cloud OnRamp for SaaS control policy to act on more of the Webex traffic handled by a router.

One benefit to using SD-AVC for DPI is that it resolves a known issue that could cause some Webex traffic to use a sub-optimal path to cloud servers. The scenario is that Webex servers in one geographical region might use some of the same IP addresses as Webex servers in a different region. In previous releases, this IP overlap could cause Webex traffic destined for one geographical region to use the edge device interface that is optimal for traffic to a different region. The traffic flow operated correctly, reaching the correct destination, but the traffic used a non-optimal path. In Cisco vManage Release 20.10.1, this is resolved.

Simplified Application-Aware Routing Policy

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, when you enable Cloud OnRamp for SaaS to operate on Webex traffic, Cisco SD-WAN Manager adds only a single sequence to application-aware routing (AAR) policies, rather than a series of sequences, as in earlier releases. Cisco Catalyst SD-WAN continues to support existing legacy AAR policies that use more sequence statements to enable Cloud OnRamp for SaaS for Webex.

If you are using a legacy AAR policy (that uses numerous sequences to enable Cloud OnRamp for SaaS for Webex traffic), disabling Webex in Cloud OnRamp for SaaS removes the series of sequences that address Webex traffic from the AAR policy. If you re-enable Webex, Cloud OnRamp for SaaS uses the newer, more efficient method of adding only a single sequence to the AAR policy.

For information about restrictions related to the new policy model, see Restrictions for the Webex Application, on page 158.

Webex Server-Side Metrics

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Webex servers can provide metrics to Cisco SD-WAN Analytics describing the the performance of different facets of Webex traffic, such as audio, video, and so on. The metrics augment the traffic metrics that Cloud OnRamp for SaaS collects using path probes to determine metrics such as loss and latency. The aggregated information from Webex servers and from probing provides a valuable tool for understanding Webex traffic performance in your network. For information about viewing the aggregated metrics, see View Details of Monitored Applications, on page 182.

Cloud OnRamp for SaaS does not use the metrics data when determining the best path for Webex traffic. See Prerequisites for Webex Server-Side Metrics, on page 155, and Enable Webex Server-Side Metrics.

Information About the SD-AVC Cloud Connector

Minimum supported release: Cisco vManage Release 20.8.1

Cisco Catalyst SD-WAN uses a component called SD-AVC Cloud Connector to collect information from Microsoft Cloud about the Microsoft application servers that handle Office 365 traffic. The information includes the transport protocols for the traffic; and the domain names, IP addresses, and ports of the application servers that manage the traffic. This server information improves the process of identifying network traffic—for example, making it possible to identify traffic from the first packet. Improving traffic identification enhances the effectiveness of application-aware routing policies because policies can often match all traffic, from the first packet.

The **SD-AVC Cloud Connector** page provides visibility into the application servers that are used for Office 365 traffic. It provides a table of the server information that Cisco Catalyst SD-WAN has collected for Office 365 traffic. For example, the table may indicate that the domains represented by *-admin.sharepoint.com correspond to Sharepoint traffic. In this case, any traffic flow with a destination domain included in those domains, such as connect-admin.sharepoint.com, can be identified as Sharepoint traffic from the first packet of the flow.

Information About Viewing Path Scores for Office 365 Traffic

Minimum supported release: Cisco vManage Release 20.8.1

For Office 365 traffic, you can view charts showing the path scores (OK, NOT-OK, or INIT) provided by Microsoft telemetry for each Microsoft service area, including Exchange, Sharepoint, and Skype. The chart shows the path scores over time for each available interface.

Viewing the path score history can be useful when troubleshooting network performance issues for Office 365 traffic—for example, to determine whether Microsoft consistently rates a particular interface as NOT-OK for some types of traffic, such as Skype traffic. If that occurs, you can investigate why the interface is consistently receiving a low path score.

Information About Configuring the Traffic Category and Service Area for Specific Policies

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

When you enable Microsoft 365 on the **Applications and Policy** page, and choose a traffic category, Cloud OnRamp for SaaS adds sequences to all application-aware routing (AAR) policies to enable Cloud OnRamp for SaaS operation on Microsoft 365 traffic, in accordance with the traffic category that you have chosen. Adding these sequences to the AAR policies enables Cloud OnRamp for SaaS operation on this traffic, with the selected traffic category.

Starting from Cisco vManage Release 20.9.1, you can edit the sequences in AAR policies individually to change the specified Microsoft 365 traffic category and service area for specific AAR policies.

Note This feature is only available for the Microsoft 365 application.

Benefits of Configuring the Traffic Category and Service Area for Specific Policies

By editing individual AAR policies, you can enable Cloud OnRamp for SaaS to operate on different Microsoft 365 service areas and traffic categories in different policies.

Information About Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

Starting from Cisco vManage Release 20.9.1, you can selectively enable Cloud OnRamp for SaaS to operate for a particular application at specific sites, while excluding other sites. When you enable an application on the **Applications and Policy** page, Cloud OnRamp for SaaS adds AAR policy sequences that match traffic for the selected application and direct the traffic in accordance with the Cloud OnRamp for SaaS best path calculation. This has the effect of enabling Cloud OnRamp for SaaS operation at all sites.

To exclude Cloud OnRamp for SaaS operation for applications at specific sites, you can edit an AAR policy and delete a specific application within the AAR policy. This disables Cloud OnRamp for SaaS activity for that application on sites that use the AAR policy.

In contrast to editing the traffic category or service area for specific policies (see Information About Configuring the Traffic Category and Service Area for Specific Policies), which works only with Microsoft 365 traffic, you can use this feature to enable or exclude any SaaS application.

Benefits of Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites

This feature enables granular, site-level control of applications that Cloud OnRamp for SaaS operates on at each site in the network.

Information About Visibility for Microsoft 365 SaaS Traffic

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Cisco vManage Release 20.9.1 introduces improved application visibility, enabling you to monitor Microsoft 365 traffic processed by Cloud OnRamp for SaaS in more detail. You can view, in graph or table formats, the volume of Microsoft 365 traffic over time, with details as to how much traffic used a direct internet access (DIA) link, and how much was routed through a gateway site. The monitoring page also shows the volume of traffic that Cloud OnRamp for SaaS does not affect.

Benefits of Visibility for Microsoft 365 SaaS traffic

Visibility into the details of how Cloud OnRamp for SaaS is routing traffic can be helpful when troubleshooting traffic routing issues.

Information About Including or Excluding Microsoft Telemetry Data from the Best Path Decision for Microsoft 365 Traffic

Minimum releases: Cisco vManage Release 20.9.1

From Cisco vManage Release 20.9.1, you can control whether the Cloud OnRamp for SaaS best path decision includes Microsoft telemetry data as a factor for Microsoft 365 traffic. When enabling telemetry for Microsoft 365 (Office 365) traffic, the **Application Feedback** dialog box contains a **Traffic Steering** check box. Check this check box to enable the use of Microsoft telemetry data in best path decisions. For information, see Enable Application Feedback Metrics for Office 365 Traffic.

Even when you elect not to use Microsoft telemetry data in best path decisions, you can view the telemetry data. You can view the telemetry data related to the Microsoft 365 application, as well as detailed information about the best path decisions made on devices, using Cisco vAnalytics. For information about Cisco SD-WAN Analytics, see Cisco vAnalytics.

For information about enabling Microsoft to provide telemetry for Microsoft 365 traffic, see Enable Microsoft to Provide Telemetry for Office 365 Traffic.

After Upgrading Cisco SD-WAN Manager

If you have enabled Microsoft telemetry on a previous release of Cisco SD-WAN Manager, and are now upgrading to Cisco vManage Release 20.9.1, Cloud OnRamp for SaaS does not automatically enable the use of Microsoft telemetry data in best path decisions. To ensure that devices use Microsoft telemetry for best path decisions, if you have configured that option, perform one of the following:

- Disable and enable Microsoft telemetry for Microsoft 365 traffic. See Enable Application Feedback Metrics for Office 365 Traffic

- Disable and enable monitoring for Microsoft 365 traffic. See Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager
- Perform the following steps:
  1. Detach and attach sites and gateways. See Configure Client Sites.
  2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
  3. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**. The **Applications and Policy** page displays all SaaS applications.
  4. Click **Save Applications and Next**. This sends the traffic steering values to devices at each site.



Note From Cisco vManage Release 20.9.1, you can enter the public system IP of edge devices, on the Microsoft portal. For details, see step 2-c under Enable Microsoft to Provide Telemetry for Office 365 Traffic.

Information About Cloud OnRamp for SaaS Support for Loopback, Dialer, and Subinterfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Cloud OnRamp for SaaS supports loopback, dialer, and subinterfaces. You can configure TLOC-extension and SIG on these interfaces.

You can configure different interfaces on a Cisco IOS XE Catalyst SD-WAN device based on your requirements. For more information about configuring network interfaces, see Configure Network Interfaces.

For more information about supported Network Address Translation (NAT) configuration on loopback and dialer interfaces, see Configure NAT.

Information About Excluding Data Prefixes

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a , Cisco Catalyst SD-WAN Manager Release 20.13.1

You can define a list of destination IP prefixes to exclude from Cloud OnRamp for SaaS optimization. You can apply a data prefix exclusion list to all SaaS applications or individually to a specific application.

A common use is to exclude the prefixes of on-premises SaaS application servers or private-cloud-hosted SaaS application servers. For example, if you have local on-premises SharePoint servers and configure Cloud OnRamp for SaaS to optimize SharePoint traffic, you can exclude the prefixes for the local SharePoint servers from Cloud OnRamp for SaaS optimization. This enables the SharePoint traffic to be routed internally, unaffected by Cloud OnRamp for SaaS.

Information About Using a Tracker for Faster Failover

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Cloud OnRamp for SaaS performs best-path determination using probes on all available interfaces. If internet connectivity on an interface fails, Cloud OnRamp for SaaS reroutes to another path, which is called failover. Detecting the failure might take some time. When relying on probes, it takes two to four minutes to detect internet connectivity failure on an interface.

To achieve a faster failover, you can configure a DIA tracker and associate it with a DIA or gateway site configured for Cloud OnRamp for SaaS. The tracker probes the transport interface periodically to determine if the internet or external network is unavailable. Associating a tracker with Cloud OnRamp for SaaS allows faster switching to an alternate path when the primary link for an application is unavailable.

The speed of a tracker or tracker group depends on the configuration of parameters such as threshold, interval, multiplier, and so on. For more information about the DIA tracker, see NAT DIA Tracker.

For information about previous support for faster failover when using Cloud OnRamp for SaaS over a SIG tunnel, see Information About Cloud OnRamp for SaaS Over SIG Tunnels, on page 188.

Benefits of Cloud onRamp for SaaS

Benefits of Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

In some network scenarios, a site connects to the internet, entirely or in part, through a gateway site that uses a VPN 0 interface to connect to the internet. This is in contrast to using service VPNs (VPN 1, VPN 2, …).

When the gateway site connects to the internet using VPN 0, the best path to cloud application servers may be through the VPN 0 interface. When Cloud onRamp for SaaS probes for the best path for the traffic of specified cloud applications, it can probe through VPN 0 interfaces at gateway sites. This extends the best path options to include more of the available interfaces connected to the internet.

Note A branch site that connects to the internet through a gateway site may also connect to the internet through one or more DIA interfaces at the branch site itself.

Benefits of Cloud onRamp for SaaS Support for Webex

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

By maintaining a list of worldwide Webex servers, and determining the best path for all available Webex servers, Cloud onRamp for SaaS provides a high degree of path optimization for Webex traffic. Even if the Webex application connects to a distant cloud server, or connects to different servers at different times, Cloud onRamp for SaaS always provides the best path to any Webex server worldwide.

Supported Devices for Cloud onRamp for SaaS

Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices support Cloud onRamp for SaaS.

The following table describes the device support for specific Cloud onRamp for SaaS features.

Table 53: Device Feature Support

Feature	Cisco IOS XE Catalyst SD-WAN Device Support	Cisco vEdge Device Support
Basic Cloud onRamp for SaaS functionality	Yes	Yes
Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites	Yes	Yes
Webex application support	Yes	No
Application Feedback Metrics for Office 365 Traffic	Yes	No
Microsoft to Provide Traffic Metrics for Office 365 Traffic	Yes	No
SD-AVC Cloud Connector	Yes	No
Viewing Path Scores for Office 365 Traffic	Yes	No
Cloud onRamp for SaaS Over SIG Tunnels	Yes	Yes
SaaS Application Lists	Yes	No
Webex Server-Side Metrics	Yes	No

For information about features supported on Cisco vEdge devices, see Cloud onRamp for SaaS, Cisco SD-WAN Release 20.3.1 and Later.

Prerequisites for Cloud OnRamp for SaaS

The following sections describe the prerequisites for Cloud OnRamp for SaaS features.

Prerequisites for Cloud OnRamp for SaaS, General

The prerequisites for using Cloud OnRamp for SaaS differ for Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices. For information about using Cloud OnRamp for SaaS with Cisco vEdge devices, see Cloud OnRamp Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20.

For Cisco IOS XE Catalyst SD-WAN devices, the requirements are:

- The devices must be running Cisco IOS XE Catalyst SD-WAN Release 17.3.1a or later.
- The devices must be in Manager mode.
- All Cisco Catalyst SD-WAN Controller instances must be in Manager mode.
- A centralized policy that includes an application-aware policy must be activated. You can configure more than one centralized policy in Cisco SD-WAN Manager, but only one can be active.

Note This is an important difference from using Cloud OnRamp for SaaS with Cisco vEdge devices, which do not have this requirement.

- Cloud OnRamp for SaaS is enabled (**Administration** > **Settings**).

  From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cloud OnRamp for SaaS is enabled by default. (**Administration** > **Settings**)

To specify traffic by Office 365 traffic category, the following are also required:

- Cisco SD-AVC is enabled (**Administration** > **Cluster Management**).
- Cisco SD-AVC Cloud Connector is enabled (**Administration** > **Settings**). If Cloud Connector is not enabled, policies specifying Office 365 traffic cannot match the Office 365 traffic. The traffic uses the default path, rather than the best path selected by Cloud OnRamp for SaaS.

Prerequisites for Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

Cloud onRamp for SaaS probing through VPN 0 interfaces at gateway sites presupposes that a branch site connects to the internet through a gateway site, and that the gateway site connects to the internet using a VPN 0 interface. The branch site may or may not also connect to the internet through one or more DIA connections.

Prerequisites for Cloud OnRamp for SaaS Support for Webex

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

- To download the latest information about Webex servers, as described in "Maintaining an Up-to-Date List of Webex Servers" in Information About Cloud OnRamp for SaaS Support for Webex, Cisco SD-WAN Manager requires access to the internet.
- When you enable Cloud OnRamp for SaaS to optimize Webex traffic, ensure that for each router, the service VPN has a default route configured. This default route is required for the Webex DNS and control traffic, which are components of Webex traffic that are not optimized by Cloud OnRamp for SaaS.
- Verify that SD-WAN Manager can reach this domain:

  https://info.net-int.infra.webex.com/v1/prefixes/regions

Prerequisites for Configuring the Traffic Category and Service Area for Specific Policies

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

- You must have multiple active AAR policies.

- To edit the service area and traffic category, you must enable **Monitoring** and **Policy/Cloud SLA** for the Microsoft 365 application. For information, see Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager.

Prerequisites for Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

Availability of multiple AAR policies associated with different sets of sites.

Prerequisites for Visibility for Microsoft 365 SaaS Traffic

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

- Enable application visibility and flow visibility. For information, see Enable Application Visibility and Flow Visibility, on page 178.
- To view the graphical visualizations of traffic, and to view logs, enable on-demand troubleshooting. For information, see On Demand Troubleshooting in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Prerequisites for Including or Excluding Microsoft Telemetry Data from the Best Path Decision for Microsoft 365 Traffic

Minimum releases: Cisco vManage Release 20.9.1

Enable Microsoft traffic metrics.

See Enable Microsoft to Provide Traffic Metrics for Office 365 Traffic.

Prerequisites for Webex Server-Side Metrics

Minimum releases: Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

- Enable SD-AVC in **Administration** > **Settings**.
- Enable Cloud Services in **Administration** > **Settings**.
- Webex account (This is usually an account for your organization).
- Enable server-side metrics. See Enable Webex Server-Side Metrics, on page 174.

Prerequisites for Cloud OnRamp for SaaS Support on Loopback, Dialer, and Subinterfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

To use a dialer interface for Cloud OnRamp for SaaS, the Point-to-Point Protocol (PPP) models associated with the DIA interface must support NAT DIA.

Prerequisites for Excluding a Data Prefix List for a Cloud OnRamp for SaaS Application

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Before using or creating a destination data prefix list for a Cloud OnRamp for SaaS application, perform the following on the **Applications and Policy** page, for the application or applications for which you are excluding specific prefixes:

- Enable monitoring for the application.
- Enable Policy/Cloud SLA for the application.

Prerequisites for Faster Failover with a DIA Tracker

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

- Configure a tracker with a DNS name or an IP address of the endpoint on the DIA or gateway site where Cloud OnRamp for SaaS is enabled.
  - To configure a DIA tracker using a Cisco System feature template, see Configure NAT DIA Tracker on IPv4 Interfaces Using Feature Templates in Cisco SD-WAN Manager.
  - Devices on the site must have a tracker or tracker group associated with them.
  - You can configure an ICMP tracker using a CLI template. For more information about configuring an ICMP tracker, see Information About NAT DIA Tracking.
- Ensure the DIA interfaces are configured for Cloud OnRamp for SaaS before associating a tracker.

Restrictions for Cloud onRamp for SaaS

The following section(s) describe the restrictions applicable to Cloud OnRamp for SaaS features.

Restrictions for Cloud OnRamp for SaaS, General

Restriction	Description
Loopback interface TLOC	Configuring Cloud OnRamp for SaaS when a site is using a loopback as a transport locator (TLOC) interface is not supported. From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cloud OnRamp for SaaS supports using loopback as a TLOC interface.

Restriction	Description
DNS server	Cloud OnRamp doesn't support if the name-server is reachable over SD-WAN tunnel (through OMP), DNS resolution will fail.
Dialer interface TLOC	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cloud OnRamp for SaaS supports using dialer as a TLOC interface. For resctrictions related to dialer interfaces, see Restrictions for Using a Dialer Interface with NAT DIA.
VLAN interface TLOC	Configuring Cloud OnRamp for SaaS when a site is using VLAN as a TLOC interface is not supported.
Cellular interface TLOC	Configuring Cloud OnRamp for SaaS when a site is using cellular as a TLOC interface is not supported.
Application-aware policy	Configuring Cloud OnRamp for SaaS on Cisco IOS XE Catalyst SD-WAN device devices is only through centralized app-aware policy using match condition "cloud-saas-app-list" and action "cloud-saas". For mixed deployments including Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices, we recommend to have different app-aware policies for Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices.
ICMP traffic	Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco SD-WAN Release 20.8.1, Cloud OnRamp for SaaS does not support ICMP traffic. This has a minor effect on Webex traffic counters, as compared with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco SD-WAN Release 20.7.1.
Configuration groups	You can configure Cloud OnRamp for SaaS using the methods described in the Configure Cloud onRamp for SaaS, on page 160 section. Cloud OnRamp for SaaS does not support configuration using configuration groups.
NAT pool	Configuring Cloud OnRamp for SaaS with NAT pool mapping on DIA interface is not supported. Configuring Cloud OnRamp for SaaS with NAT pool mapping on DIA interface is supported from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and later.

Restrictions for Service VPN Gateway Mode

When you change the VPN settings of the service-VPN DIA interface, and Cloud OnRamp for SaaS is running in service-VPN Gateway mode, Cloud OnRamp for SaaS fails to work with the new service-VPN settings. The system continues to display stale data from the previous service-VPN setting for up to 10 minutes following the change and there is no data for the new service-VPN settings.

To prevent the issue, perform the following steps:

1. Detach the site from Cloud OnRamp for SaaS sites.

2. Update the VPN settings for the desired DIA interface on the Interface Configuration page.
3. Re-attach the site to Cloud OnRamp for SaaS as a service-VPN Gateway site.

Restrictions for the Webex Application

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, when you enable Cloud OnRamp for SaaS to operate on Webex traffic, Cisco SD-WAN Manager uses a more efficient policy model, while still supporting existing legacy control policies that enable Cloud OnRamp for SaaS for Webex. If you disable the Webex application in Cloud OnRamp for SaaS, and then re-enable the Webex application, Cisco SD-WAN Manager can only use the newer policy model. Before disabling and then re-enabling the Webex application, ensure that devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.10.1a or later, and that SD-AVC is enabled (in **Administration** > **Settings**).

Restrictions for Associating a Tracker with DIA and Gateway Sites

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

You can associate a tracker with a gateway site only if connectivity to the gateway site uses VPN 0, not a service VPN.

Use Cases for Cloud onRamp for SaaS

Use Cases for Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

Enable gateway probing through VPN 0 interfaces if the following conditions apply:

- A branch site connects to the internet through a gateway site. The branch site may or may not also connect to the internet through one or more DIA interfaces.
- The gateway site has internet exits that use the transport VPN (VPN 0) through one or more interfaces.

Use Cases for the SD-AVC Cloud Connector

Minimum supported release: Cisco vManage Release 20.8.1

Visibility into server information is helpful when troubleshooting. For example, after creating a policy that applies Cloud onRamp for SaaS only to Office 365 traffic in the Sharepoint service area, you might find that Cisco Catalyst SD-WAN is not routing the first few flows of Sharepoint traffic on the best path determined by Cloud OnRamp for SaaS, and Sharepoint performance is below expectations.

To troubleshoot, you can do the following:

1. Determine which server the Sharepoint traffic is using.
2. Open the SD-AVC Cloud Connector page and filter for the term, “sharepoint”.

3. Look for the Sharepoint server you found in the first step. If that server does not appear in the list, it means that Cloud OnRamp for SaaS is not classifying the traffic to that server as Sharepoint traffic. If it is not classified as Sharepoint traffic, it does not use the best path determined by Cloud OnRamp for SaaS for the first few flows.

Use Case for Configuring the Traffic Category and Service Area

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

An organization relies heavily on Microsoft 365 for its office applications and has configured Cloud OnRamp for SaaS to optimize Microsoft 365 traffic at its headquarters and at each branch office. In addition, it uses an on-premises Outlook server at a data center to handle its company email.

Microsoft distinguishes different types of Microsoft 365 traffic using the following service areas:

- Common: Microsoft 365 ProPlus, Office in a browser, Azure Active Directory (AD), and other common network endpoints
- Exchange: Exchange Online and Exchange Online Protection
- SharePoint: SharePoint Online and OneDrive for Business
- Skype: Skype for Business and Microsoft Teams

Because the organization uses an on-premises Outlook server, the network administrator chooses to exclude Outlook traffic from the Cloud OnRamp for SaaS optimization of Microsoft 365 traffic. By modifying the AAR policies, they exclude the Exchange service area (for Outlook) from the Microsoft 365 traffic that Cloud OnRamp for SaaS operates on, thereby ensuring the best performance for the email traffic using the on-premises Outlook server.

Use Case for Enabling Specific Applications at Specific Sites

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

An organization's network spans numerous sites. Most of the sites utilize the Box.com cloud storage application, but a subset of sites does not use Box.com.

First, the network administrator creates an AAR policy that serves the subset of sites that do not use Box.com. Next, the network administrator enables Cloud OnRamp for SaaS for Box.com traffic, which enables Cloud OnRamp for SaaS operation at all sites in the network.

To exclude the subset of sites that do not use Box.com, the network administrator edits the AAR policy for that subset of sites, to disable Cloud OnRamp for SaaS operation for Box.com traffic. This has the effect of disabling Cloud OnRamp for SaaS operation for Box.com traffic at that subset of sites only.

Use Case for Excluding Data Prefixes from Cloud OnRamp for SaaS Optimization

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Some organizations host SaaS applications in private data centers that are reachable only through the organization's internal network. If you enable Cloud OnRamp for SaaS to optimize traffic for one of these SaaS applications, then Cloud OnRamp for SaaS might attempt to route the SaaS traffic to a server outside

the organization's internal network. This inadvertently prevents the SaaS traffic from reaching the private data center.

For example, an organization hosts a private on-premises SharePoint server for its internal SharePoint traffic. At the same time, the organization has enabled Cloud OnRamp for SaaS optimization for several SaaS applications, including SharePoint. This can inadvertently interfere with the SharePoint traffic.

To prevent Cloud OnRamp for SaaS optimization of the internal SharePoint traffic, network administrators configure Cloud OnRamp for SaaS to exclude the IP prefixes of the internal SharePoint servers. Consequently, internal SharePoint traffic flows correctly to the on-premises SharePoint server at the private data center.

Configure Cloud onRamp for SaaS

The following sections describe configuration procedures for Cloud OnRamp for SaaS features.

Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices

You can enable Cloud OnRamp for SaaS in your Cisco Catalyst SD-WAN overlay network on sites with Direct Internet Access (DIA) and on DIA sites that access the internet. You can also enable Cloud OnRamp for SaaS on client sites that access the internet through another site in the overlay network, called a gateway site. Gateway sites can include regional data centers or carrier-neutral facilities. When you enable Cloud OnRamp for SaaS on a client site that accesses the internet through a gateway, you also enable Cloud OnRamp for SaaS on the gateway site.



Note You can only enable Cloud OnRamp for SaaS features using the Cisco SD-WAN Manager procedures described in this document. We do not support configuring Cloud OnRamp for SaaS using CLI templates. Even when you configure other features on a device using a CLI template, you must nevertheless use Cisco SD-WAN Manager for configuring Cloud OnRamp for SaaS features.

Enable Cloud OnRamp for SaaS

Before You Begin

From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cloud OnRamp for SaaS is enabled by default.

Enable Cloud OnRamp for SaaS

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud OnRamp for SaaS**.
3. In the **Cloud OnRamp for SaaS** field, click **Enabled**.
4. Click **Save**.

Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager

1. Open Cloud OnRamp for SaaS.
   - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     or

   - In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** window displays all SaaS applications.
3. Optionally, you can filter the list of applications by clicking an option in the **App Type** field.
   - **Standard**: Applications included by default for Cloud OnRamp for SaaS.
   - **Custom**: User-defined SaaS application lists (see Information About SaaS Application Lists).
4. (Optional) (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) To exclude specific data prefixes for all SaaS applications, click **Exclude Destination Data Prefix**.

   In the drop-down list, choose an existing data prefix list or click **New Data Prefix List** to define a new data prefix list.

   For more information about configuring a data prefix, see the Configure Data Prefix section in Centralized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.



Note To exclude data prefixes for a specific SaaS application, see a later step in this procedure.

   For information about excluding data prefixes, see Information About Excluding Data Prefixes, on page 151.
5. Enable applications and configure.

Column	Description
Applications	Applications that can be used with Cloud OnRamp for SaaS. If you enable the **Office 365** application, you can click the **Enable Application Feedback** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Microsoft. For information, see Enable Application Feedback Metrics for Office 365 Traffic. If you enable the **Webex** application, you can click the **Enable Application Telemetry** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Webex. **Note** Enabling application feedback metrics opens a Microsoft site that requests various permissions to access your application telemetry data. These permissions enable Cisco Catalyst SD-WAN to receive application telemetry data from Microsoft and correlate it with network telemetry data. This is part of the process of computing best paths to optimally route Microsoft 365 traffic. The Bcos.IsvPartner permission provides access to the Branch Connect Web Services APIs, which Cisco uses to manage opt-in, get connectivity information about branch sites, and store location information, such as IP addresses. These APIs enable correlating traffic to branch sites. The Bcos.ReadOnly and Bcos.ReadWrite permissions are storage permissions for the tenant-specific portion of the Branch Connect Optics Store. This is an Azure storage located in the region that you select when opting in. Cisco and Microsoft use this storage location to exchange telemetry information for processing.
Monitoring	**Enabled**: Enables Cloud OnRamp for SaaS to initiate the Quality of Experience probing to find the best path. **Disabled**: Cloud OnRamp for SaaS stops the Quality of Experience probing for this application.
VPN	(Cisco vEdge devices) Specify one or more VPNs.

Column	Description
Policy/Cloud SLA	(Cisco IOS XE Catalyst SD-WAN devices) Select **Enable** to enable Cloud OnRamp for SaaS to use the best path for this application. **Note** You can select **Enable** only if there is a centralized policy that includes an application-aware policy has been activated.
	(Cisco IOS XE Catalyst SD-WAN devices) For Microsoft 365 (M365), select one of the following to specify which types of M365 traffic to include for best path determination: • **Optimize**: Include only M365 traffic categorized by Microsoft as "optimize" – the traffic most sensitive to network performance, latency, and availability. • **Optimize and Allow**: Include only M365 traffic categorized by Microsoft as "Optimize" or "Allow". The "Allow" category of traffic is less sensitive to network performance and latency than the "Optimize" category. • **All**: Include all M365 traffic.
	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can choose the service area that your M365 application belongs to. This allows you to apply the policy to only those applications in the specified service area. Microsoft allows the following service area options: • **Common**: M365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints. • **Exchange**: Exchange Online and Exchange Online Protection. • **SharePoint**: SharePoint Online and OneDrive for Business. • **Skype**: Skype for Business and Microsoft Teams. See the Microsoft documentation for information about updates to the service areas.

Column	Description
Exclude Destination Data Prefix	(Optional) From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can exclude a data prefix list for a specific SaaS application: **a.** Click **Select Destination Data Prefix**. **b.** In the drop-down list, choose a data prefix list or click **New Data Prefix List** to define a new list. **c.** Click **Save**. **Note** To exclude data prefixes for all SaaS applications, see a previous step in this procedure. For information about excluding data prefixes, see Information About Excluding Data Prefixes, on page 151.

6. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** window appears, showing the application-aware policy for the current active centralized policy.

   - You can select the application-aware policy and click **Review and Edit** to view the policy details. The match conditions of the policy show the SaaS applications for which monitoring has been enabled.
   - For an existing policy, you cannot edit the site list or VPN list.
   - You can create a new policy for sites that are not included in existing centralized policies. If you create a new policy, you must add a VPN list for the policy.
   - You can delete one or more new sequences that have been added for the SaaS applications, or change the order of the sequences.

7. Click **Save Policy and Next**. This saves the policy to the Cisco Catalyst SD-WAN Controller.
8. To activate the modified policy, click **Activate**.



Note You can choose a simple workflow under application and SLA priority to create a data prefix using exclusion of RFC1918 data prefix lists (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). When you switch from already created simple workflow to advanced workflow layout, you can see the default RFC1918 data prefix list sequences in proper order and can proceed to add any additional prefix lists on top of that.

Configure Sites for Cloud onRamp for SaaS Using Cisco SD-WAN Manager

Configure two types of sites:

- Client sites
- Direct internet access (DIA) sites

Configure Client Sites

To configure Cloud OnRamp for SaaS on client sites that access the internet through gateways, configure Cloud OnRamp for SaaS both on the client sites and on the gateway sites.

Note You cannot configure Cloud OnRamp for SaaS with Point-to-Point Protocol (PPP) interface on the gateway sites.

Client sites in the Cloud OnRamp service choose the best gateway site for each application to use for accessing the internet.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**. The **Cloud OnRamp for SaaS** Dashboard appears.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Client Sites**. The page displays the following elements:
   - Attach Sites: Add client sites to Cloud OnRamp for SaaS service.
   - Detach Sites: Remove client sites from Cloud OnRamp for SaaS service.
   - Client sites table: Display client sites configured for Cloud OnRamp for SaaS service.
3. On the **Cloud OnRamp for SaaS** > **Manage Sites** window, click **Attach Sites**. The **Attach Sites** dialog box displays all sites in the overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in Manager mode.
4. Choose one or more client sites from **Available Sites** and move them to **Selected Sites**.
5. Click **Attach**. The Cisco SD-WAN Manager saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
6. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS** to return to the Cloud OnRamp for SaaS Dashboard screen.
7. Click **Manage Cloud OnRamp for SaaS** and choose **Gateways**. The page displays the following elements:
   - Attach Gateways: Attach gateway sites.
   - Detach Gateways: Remove gateway sites from the Cloud OnRamp service.
   - Edit Gateways: Edit interfaces on gateway sites.
   - Gateways table: Display gateway sites configured for Cloud OnRamp service.
8. In the **Manage Gateways** window, click **Attach Gateways**. The **Attach Gateways** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in Manager mode.
9. In the **Device Class** field, choose one of the following operating systems:
   - **Cisco OS**: Cisco IOS XE Catalyst SD-WAN devices
   - **Viptela OS (vEdge)**: Cisco vEdge devices

10. Choose one or more gateway sites from **Available Sites** and move them to **Selected Sites**.
11. (Cisco vEdge devices for releases before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a) To specify GRE interfaces for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

    (Cisco vEdge devices for releases from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a) To specify the VPN 0 interfaces or service VPN interfaces in gateway sites for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.



Note If you do not specify interfaces for Cloud OnRamp for SaaS to use, the system selects a NAT-enabled physical interface from VPN 0.

    a. Click **Add interfaces** to selected sites (optional), located in the bottom-right corner of the **Attach Gateways** window.
    b. Click **Select Interfaces**.
    c. From the available interfaces, choose the GRE interfaces to add (for releases before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a), or the VPN 0 interfaces or service VPN interfaces to add (for releases from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a).
    d. Click **Save Changes**.

12. (Cisco IOS XE Catalyst SD-WAN devices) To configure the routers at a gateway site, perform the following steps.



Note If you don't specify interfaces for Cloud OnRamp for SaaS, an error message indicates that the interfaces aren't VPN 0.

    a. Click **Add interfaces to selected sites**.
    b. The **Attach Gateways** window shows each WAN edge router at the gateway site.

       Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, you can choose Service VPN or VPN 0 if the gateway uses Cisco IOS XE Catalyst SD-WAN devices.

       - If the routers at the gateway site connect to the internet using service VPN connections (VPN 1, VPN 2, …), choose **Service VPN**.
       - If the routers at the gateway site connect to the internet using VPN 0, choose **VPN 0**.



Note

- Correctly choosing **Service VPN** or **VPN 0** requires information about how the gateway site connects to the internet.
- All WAN edge routers at the gateway site must use either service VPN or VPN 0 connections for internet access. Cloud OnRamp for SaaS does not support a mix of both.

    c. Do one of the following:

- If you chose **Service VPN**, then for each WAN edge router, choose the interfaces to use for internet connectivity.
- If you chose **VPN 0**, then either choose **All DIA TLOC**, or choose **TLOC list** and specify the colors to include in the TLOC list.

d. From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you chose **All DIA TLOC**, or **TLOC list** and specified the colors to include in the TLOC list, you can associate a tracker or tracker group for the gateway site by checking the **Enable Tracker Association** check box.

For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 156.

e. To enable load balancing for cloud application traffic across multiple interfaces on the WAN edge device, check the **Enable Load Balancing** check box. (See Load Balancing Across Multiple Interfaces.)

f. Configure the load-balancing options:

Option	Description
Loss (%)	After determining the best path interface for a cloud application, Cloud OnRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than this configured value. You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface. For example, if the best path interface has a packet loss value of 2% and the **Loss** value is 10, then another interface can be used for load balancing only if its packet loss value is no more than 12%. Range: 0 to 100 Default: 10
Latency (milliseconds)	To use another interface for load balancing, the latency value of the interface can't vary from the latency of the best path interface by more than this number of milliseconds. You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface. For example, if the best path interface has a latency of 5 milliseconds, and the **Latency** value is set to 50, then another interface can be used for load balancing only if its latency is no more than 55 milliseconds. Range: 1 to 1000 Default: 50

Option	Description
Source IP based Load Balancing	To ensure that all traffic from a single host uses a single interface, enable this option. For example, to ensure that DNS and application traffic use the same path, enable this option.

g. Click **Save Changes**.

13. Click **Attach**. Cisco SD-WAN Manager saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
14. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

Edit Interfaces on Gateway Sites

1. Select the sites you want to edit and click **Edit Gateways**.
2. In the **Edit Interfaces of Selected Sites** window, select a site to edit.
   - Choose **Service VPN** or **VPN 0** based on how the gateway site connects to the internet.
   - Do one of the following:
     - If you chose **Service VPN**, then for each WAN edge router, choose the interfaces to use for internet connectivity.
     - If you chose **VPN 0**, then either choose **All DIA TLOC**, or choose **TLOC list** and specify the colors to include in the TLOC list.
   - From Cisco Catalyst SD-WAN Manager Release 20.13.1, when you choose **VPN 0**, you can associate a tracker with the gateway sites by checking the **Enable Tracker Association** check box.

     For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 156.
   - To add interfaces, click the **Interfaces** field to select available interfaces.
   - To remove an interface, click the **X** beside its name.
   - To enable load balancing for cloud application traffic across multiple interfaces on the WAN edge device, check the **Enable Load Balancing** check box, and configure the load balancing options. (See Load Balancing Across Multiple Interfaces, on page 144.)

Option	Description
Loss (%)	After determining the best path interface for a cloud application, Cloud OnRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than this configured value. You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface. For example, if the best path interface has a packet loss value of 2% and the **Loss** value is 10, then another interface can be used for load balancing only if its packet loss value is no more than 12%. Range: 0 to 100 Default: 10
Latency (milliseconds)	To use another interface for load balancing, the latency value of the interface cannot vary from the latency of the best path interface by more than this number of milliseconds. You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface. For example, if the best path interface has a latency of 5 milliseconds, and the **Latency** value is set to 50, then another interface can be used for load balancing only if its latency is no more than 55 milliseconds. Range: 1 to 1000 Default: 50
Source IP based Load Balancing	To ensure that all traffic from a single host uses a single interface, enable this option. For example, to ensure that DNS and application traffic use the same path, enable this option.

3. Click **Save Changes** to push the template to the device(s).

Configure Direct Internet Access (DIA) Sites

Note Cloud OnRamp for SaaS requires an SD-WAN tunnel to each physical interface to enable SaaS probing through the interface. For a physical interface configured for DIA only, without any SD-WAN tunnels going to the SD-WAN fabric, configure a tunnel interface with a default or any dummy color in order to enable use of Cloud OnRamp for SaaS. Without a tunnel interface and color configured, no SaaS probing can occur on a DIA-only physical interface.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. From the **Manage Cloud OnRamp for SaaS** drop-down list, located to the right of the title bar, choose **Direct Internet Access (DIA) Sites**.

   The **Manage DIA**window provides options to attach, detach, or edit DIA sites, and shows a table of sites configured for the Cloud OnRamp service.
3. Click **Attach DIA Sites**. The **Attach DIA Sites** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in Manager mode.
4. In the **Device Class** field, select one of the following:
   - **Cisco OS**: Cisco IOS XE Catalyst SD-WAN devices
   - **Viptela OS (vEdge)**: Cisco vEdge devices
5. Choose one or more DIA sites from **Available Sites** and move them to **Selected Sites**.
6. (For Cisco vEdge devices) By default, if you don't specify interfaces for Cloud OnRamp for SaaS to use, the system selects all NAT-enabled physical interfaces from VPN 0. Use the following steps to specify particular interfaces for Cloud OnRamp for SaaS.

Note You can't select a loopback interface.

   a. Click the link, **Add interfaces to selected sites** (optional), located in the bottom-right corner of the window.
   b. In the **Select Interfaces** drop-down list, choose interfaces to add.
   c. Click **Save Changes**.
7. (For Cisco IOS XE Catalyst SD-WAN devices, optional) Specify TLOCs for a site.

Note Configuring Cloud OnRamp for SaaS when using a loopback as a TLOC interface is not supported.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cloud OnRamp for SaaS supports using loopback as a TLOC interface.

Note If you do not specify TLOCs, the **All DIA TLOC** option is used by default.

a. Click the **Add TLOC to selected sites** link at the bottom-right corner of the **Attach DIA Sites** dialog box.

b. In the **Edit Interfaces of Selected Sites** dialog box, choose **All DIA TLOC**, or **TLOC List** and specify a TLOC list.

c. From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you chose **All DIA TLOC**, or **TLOC list** and specified the colors to include in the TLOC list, you can associate a tracker or tracker group for the DIA site by checking the **Enable Tracker Association** check box.

For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 156.

d. Click **Save Changes**.

8. Click **Attach**. The Cisco SD-WAN Manager NMS saves the feature template configuration to the devices. The **Task View** window displays a Validation Success message.
9. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

Edit Interfaces on Direct Internet Access (DIA) Sites

1. Select the sites to edit and click **Edit DIA Sites**.
2. (Cisco vEdge devices) On the **Edit Interfaces of Selected Sites** screen, select a site to edit.
   - To add interfaces, click the **Interfaces** field to select available interfaces.
   - To remove an interface, click the **X** beside its name.
3. (Cisco IOS XE Catalyst SD-WAN devices) In the **Edit Interfaces of Selected Sites** dialog box, do the following:

a. Click **All DIA TLOC** to include all TLOCs, or click **TLOC List** to select specific TLOCs.

b. From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can associate a tracker on DIA sites by checking the **Enable Tracker Association** check box.

For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 156.

4. Click **Save Changes** to push the new template to the devices.

To return to the Cloud OnRamp for SaaS Dashboard, select **Configuration** > **Cloud OnRamp for SaaS**.

Enable Application Feedback Metrics for Office 365 Traffic

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can enable the following types of application feedback from additional sources. Cloud OnRamp for SaaS can use these metrics to help determine the best path for Office 365 traffic. See Best path determination, on page 144.

- Enable telemetry with Microsoft Exchange cloud servers, which can provide best path metrics for Office 365 traffic on specifically configured interfaces. This involves use of a Microsoft service called Microsoft 365 informed network routing. To understand this feature better, see the information available in the Microsoft 365 informed network routing document.
- Enable application response time (ART) metrics, which configures network devices to report ART metrics.

Before You Begin

- Enable monitoring for Office 365 traffic.

  See Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 161.
- Configure a policy for Office 365, for Cisco IOS XE SD-WAN devices.

  See the Policy/Cloud SLA options in Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 161.
- To enable NetFlow metrics, enable Cloud Services.

  (From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Services**)
- To enable NetFlow metrics for devices in the network, enable the **NetFlow** and **Application** options in the localized policy for each device.

  (From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies** > **Localized Policy** > **Policy template**, **Policy Settings** section)
- Enable Cisco SD-WAN Analytics. See Cisco vAnalytics Insights.

Enable Application Feedback Metrics for Office 365 Traffic

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.
3. In the **Office 365** row, click the **Enable Application Feedback for Path Selection** link.

   The **Application Feedback** dialog box opens.
4. In the **Application Feedback** dialog box, enable traffic metrics:
   - **Telemetry**: Enable Telemetry with Microsoft Exchange cloud servers to receive traffic metrics for Office 365 traffic over specific configured interfaces. For information about configuring interfaces for these metrics, see Enable Microsoft to Provide Telemetry for Office 365 Traffic, on page 173.

     If the option is disabled and the dialog box shows a message requesting sign-in to a Microsoft account, copy the code provided in the message and click the link to sign in. Provide the code on the Microsoft page that is displayed and log in with your Microsoft tenant account credentials when prompted. After signing in, the **Telemetry** option in the dialog box is enabled.

See Enable Microsoft to Provide Telemetry for Office 365 Traffic, on page 173.

- **Traffic Steering**: From Cisco vManage Release 20.9.1, check this check box to allow Cloud OnRamp for SaaS to factor in the Microsoft telemetry data in the best path decision. If you disable this, you can still view the Microsoft telemetry data in the Cisco SD-WAN Analytics dashboard, but the telemetry does not affect the best path decision.
- (Optional) **Application Response Time (ART)**: Enable ART metrics.



Note Enabling ART automatically configures devices to report ART metrics.

5. Click **Save**.

Enable Microsoft to Provide Telemetry for Office 365 Traffic

You can enable Microsoft Exchange cloud servers to calculate traffic metrics for Microsoft Exchange traffic coming from specific interfaces in the Cisco Catalyst SD-WAN overlay. Using the Microsoft Azure portal, you specify which interfaces to include, indicating the interfaces by their public IP addresses. This is called opting in the interfaces.

For the specified interfaces, Microsoft identifies the Office 365 traffic by packet source ID and provides metrics that Cloud OnRamp for SaaS can use to determine the best path for the Office 365 traffic.

Before You Begin

- Enable Cloud OnRamp for SaaS

  (**Administration** > **Settings** > **Cloud OnRamp for SaaS**)

  From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cloud OnRamp for SaaS is enabled by default.

- Enable SD-AVC Cloud Connector

  (**Administration** > **Settings** > **SD-AVC Cloud Connector**)

  Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

  Administration > **Settings** > **SD-AVC**

  See Enable Cisco SD-AVC Cloud Connector.

- Enable Cloud Services

  (**Administration** > **Settings** > **Cloud Services**)

- Configure statistics collection interval to 5 minutes.

  (**Administration** > **Settings** > **Statistics Configuration**)

- Enable Microsoft telemetry for Office 365 traffic. See Enable Application Feedback Metrics for Office 365 Traffic, on page 172.
- Activate the Microsoft 365 informed network routing service for your Microsoft 365 tenant account.
- **ip visibility**

To enable telemetry to operate, configure **ip visibility** on each Cisco IOS XE Catalyst SD-WAN device in the network, as follows:

```
policy
app-visibility
ip visibility features
  cxp        enable
  probe-saas enable
```

Enable Microsoft to Provide Telemetry for Office 365 Traffic

Note The functionality of the Microsoft Azure portal is subject to change and is therefore outside the scope of this documentation. These high-level instructions provide some guidance, but see Microsoft 365 documentation for details.

For information about the following steps, see the "Microsoft 365 informed network routing" topic in the Microsoft 365 documentation.

1. Log in to the Microsoft Azure portal. (For information about how to create a Microsoft Azure tenant account, see the Microsoft Azure documentation.)
2. Using the Microsoft Azure portal, specify Cisco Catalyst SD-WAN overlay network interfaces for which to track traffic metrics.
   a. In the Azure portal, access the Microsoft 365 admin center.
   b. On the **Locations** page, add a location entry for each location in the SD-WAN overlay network, as desired.
   c. Within a location entry, do one of the following:
      - For locations using an edge router operating with Cisco IOS XE Release 17.9.1a or later, on the "Add an office location" page (or the equivalent), enable the option to allow an SD-WAN solution to automatically set the LAN subnet and egress address range. Then enter the system IP address of the edge device for the location.
      - For locations using an edge router operating with Cisco IOS XE Release 17.8.x or earlier, add egress IP addresses, using the public IP address of the desired interfaces.

Enable Webex for Cloud OnRamp for SaaS

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

To enable Cloud onRamp for SaaS to determine the best path for Webex traffic, enable the Webex application in the same way as other applications. See Enable Cloud OnRamp for SaaS, Cisco IOS XE SD-WAN Devices.

Enable Webex Server-Side Metrics

Minimum releases: Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Before You Begin

To enable telemetry to operate, configure **ip visibility** on each Cisco IOS XE Catalyst SD-WAN device in the network, as follows:

```
policy
app-visibility
ip visibility features
  cxp        enable
  probe-saas enable
```

Enable Webex Server-Side Metrics

Webex integrations enable an application, such as Cisco SD-WAN Manager, to request information from Webex servers, using an application programming interface (API).

1. Using your Webex account, create an integration for Cisco SD-WAN Manager. For information about creating the integration, see Webex for Developers documentation, Integrations & Authorization.

   Creating the Webex integration requires a redirect URI, which includes the IP address of your Cisco SD-WAN Manager server, in the following format:

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect

   At the end of the process of creating the Webex integration, the Webex for Developers site provides you with a client ID and client secret.

Note The details for creating an integration app in the Webex for Developers site are beyond the scope of this document.

2. When you enable Webex in Cloud OnRamp for SaaS, use the client ID and client secret that you received in the previous step to enable Cisco SD-WAN Manager to use the WebEx integration.

   a. Open Cloud OnRamp for SaaS:

      - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

        Or

      - In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

   b. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

      The **Applications and Policy** page displays the Cloud OnRamp applications.

   c. Adjacent to **Webex**, click **Enable vAnalytics Webex Telemetry**.

   d. In the pop-up window, check the **Enable Webex Telemetry** checkbox.

   e. Enter the client ID and client secret for the Webex integration, and click **Save**.

   f. When prompted, enter your **Webex** account credentials.

Note You must use the credentials for the Webex account associated with the Webex integration you used in the previous step. This enables Webex telemetry for that Webex account.

g. Click **Save Applications and Next** to save the Webex telemetry configuration on Cisco SD-WAN Manager and push the updates to edge devices and to Cisco SD-WAN Analytics.

Update the Webex Server Information for Cloud OnRamp for SaaS

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for SaaS** to display the Cloud OnRamp for SaaS dashboard.
2. (This step applies only to releases earlier than Cisco vManage Release 20.10.1.) If the dashboard shows a dialog box prompting you to synchronize Webex server information, click **Yes** in the dialog box.

   Cisco SD-WAN Manager displays the **Application Aware Routing Policy** page, enabling you to review the policy. The policy includes updated match conditions that use the latest Webex server information.
3. Click **Save Policy**.

   Cloud OnRamp for SaaS updates the following, as needed, to reflect the updated information for Webex servers worldwide:

   - Match conditions in the application-aware policy
   - Configuration for probing the cloud application

Configure the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

Before You Begin

To edit the service area and traffic category, you must enable **Monitoring** and **Policy/Cloud SLA** for the Microsoft 365 application with a minimum of one service area. For information, see Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager.

Configure the Traffic Category and Service Area

1. Open Cloud OnRamp for SaaS.
   - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     Or
   - In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** page displays all the Cloud OnRamp for SaaS applications.

3. Click the edit icon from the **Policy/Cloud SLA** column for the Microsoft 365 application.

   The **Policy/Cloud SLA Settings** pop-up window opens.

4. Perform one of the following in the **Policy/Cloud SLA Settings** pop-up window.

   - Click **Yes**. Select a minimum of one service area and traffic category.
   - If you have already selected a service area and traffic category, click **No** and edit the Microsoft 365 categories or service area.

5. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page opens. A list of AAR policies in the current active centralized policy appears.

6. Select the AAR policy that you wish to edit and click **Review and Edit**.

   The **Review Policy** page opens.

7. Select the Microsoft 365 sequence you wish to edit, to change the service area or traffic category, and click the edit icon.

8. Edit the service area and traffic category, and click **Save Match And Actions**.

9. Click **Save Policy and Next**. This saves the policy.

Configure AAR Policy to Enable Cloud OnRamp Operation on Specific Applications at Specific Sites Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

1. Open Cloud OnRamp for SaaS.

   - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     Or

   - In Cisco SD-WAN Manager menu, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** page displays all the Cloud OnRamp for SaaS applications.

3. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page opens, showing the application-aware policies in the current active centralized policy.

4. Select the policy you wish to edit and click **Review and Edit** to view the policy details.

5. You can now delete one or more sequences that have been added by Cloud OnRamp for SaaS for specific applications or change the order of the sequences.

6. Click **Save Policy and Next**. This pushes the updated policy to the Cisco SD-WAN Controller.

Note Note: When you enable an application on the **Applications and Policy** page, by default, Cloud OnRamp for SaaS is enabled for all AAR policies that are part of the current active centralized policy.

Enable Application Visibility and Flow Visibility

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Enable Visibility and Flow Visibility Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Continue clicking **Next** until the **Policy Settings** page appears.
5. Check the **Netflow and Applications** check box.
6. Click **Save Policy**.

   Application visibility and flow visibility are now enabled.

Enable Application Visibility and Flow Visibility Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Configure Visibility for Microsoft 365 SaaS traffic Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Enable a Device to Provide Data for the Visualization of Microsoft 365 Traffic

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. The **On Demand Troubleshooting** page opens.
2. Click the **Select Device** drop-down list and choose a device.
3. Click the **Select Data Type** drop-down list and choose the data type **DPI**.
4. Select a time range from **Data Backfill Time Period**.
5. Click **Add** to queue the device for processing.
6. Wait until the **Status** column shows **Completed**.

View Application Usage

Minimum releases (for Microsoft 365 traffic): Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Minimum releases (for Webex traffic): Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

1. Open Cloud OnRamp for SaaS.
   - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     Or

   - In Cisco SD-WAN Manager, click the cloud icon near the top right and select **Cloud OnRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS**.
3. Click the **Microsoft 365** application or the **Webex** application. A list of devices that are attached to a DIA or gateway is shown.
4. In the **Application Usage** column of a device, click **View Usage**.

   For the Webex application, the usage information is shown according to Webex region.
5. The **CoR SaaS Application Usage** page displays the information for each type of traffic. To limit the traffic information that is displayed, click the **Search** field, and choose **All CoR SaaS Traffic**, **DIA**, **Gateway**, or **Non CoR SaaS**.

Note

- The information presented in the above graphs or logs is for an individual device. You can view the information related to only one device at a time. The graphs or logs are only shown for those devices for which on-demand troubleshooting is enabled. For information about on-demand troubleshooting, see On-Demand Troubleshooting.
- IP visibility feature commands are supported only through CLI or add-on CLI template.
- If you don't see any application usage for each type of traffic for a particular Cisco IOS XE Catalyst SD-WAN device, add the following configuration to the device using a CLI add-on feature template:

```
policy
 app-visibility
 ip visibility features
  cxp        enable
  probe-saas enable
```

Verify Cloud onRamp for SaaS

The following section(s) describe the procedures for verifying Cloud OnRamp for SaaS features.

Verify That an Application is Enabled for Cloud OnRamp for SaaS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Applications and Policy**.

   The **Applications and Policy** window displays all SaaS applications.
3. In the row of the application that you are verifying, check that the **Monitoring** column and the **Policy/Cloud SLA** column both show **Enabled**.

Verify Changes to the Configuration of the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   A list of devices is displayed.
3. For the device you wish to verify, click **…** and click **Running Configuration**. The **Running Configuration** window opens, displaying the running configuration.
4. Verify that the running configuration reflects any changes that you have made to AAR policies.

Or

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

   The **Policies** page displays the policies.
2. For the policy, you wish to verify, click **…** and click **Preview**.

   The **Policy Configuration Preview** pop-up window appears, providing a preview of the running configuration.
3. Verify that the policy preview reflects any changes that you have made to AAR policies.

Verify Which Applications Are Enabled for Specific Devices Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

A list of devices is displayed.

3. For the device you wish to verify, click **…** and click **Running Configuration**. The **Running Configuration** window opens, displaying the running configuration.
4. Verify that the running configuration reflects any changes that you have made to AAR policies.

Verify Which Applications Are Enabled for a Specific Policy Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

   The **Policies** window displays the policies.
2. For the policy, you wish to verify, click **…** and click **Preview**.

   The **Policy Configuration Preview** page appears, providing a preview of the running configuration.
3. Verify that the policy reflects any changes that you have made to AAR policies.

Verify the Excluded Data Prefixes Using Cisco SD-WAN Manager

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

Before You Begin

You can exclude specific data prefixes from Cloud OnRamp for SaaS optimization. For information, see Information About Excluding Data Prefixes, on page 151. The excluded data prefixes appear in the application-aware routing policy. This procedure displays the application-aware routing policy, enabling you to verify the excluded data prefixes.

Verify Excluded Prefixes

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Applications and Policy**.

   The **Applications and Policy** page displays all SaaS applications.
3. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page appears, showing the application-aware policies for the active centralized policies.
4. Choose an application-aware policy and click **Review and Edit** to view the policy details.
5. Click **Preview**.
6. Click **Config Diff**.

7. View the data prefixes that you are excluding.

Monitor Cloud onRamp for SaaS

The following section(s) describe the procedures for monitoring Cloud OnRamp for SaaS features.

View Details of Monitored Applications

1. Open Cloud OnRamp for SaaS.
   - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     or

   - In Cisco SD-WAN Manager, click the cloud icon at the top right and click **Cloud OnRamp for SaaS**.

   The page includes a tile for each monitored application, with the following information:
   - How many sites are operating with Cloud OnRamp for SaaS.
   - A color-coded rating of the Quality of Experience (vQoE) score for the application (green=good score, yellow=moderate score, red=poor score) on the devices operating at each site.

2. Optionally, you can click a tile to show details of Cloud OnRamp for SaaS activity for the application, including the following:

Field	Description
vQoE Status	A green checkmark indicates that the vQoE score for the best path meets the criteria of an acceptable connection. The vQoE is calculated based on average loss and average latency. For Office 365 traffic, other connection metrics are also factored in to the vQoE score.

Field	Description
vQoE Score	For each site, this is the vQoE score of the best available path for the cloud application traffic. The vQoE score is determined by the Cloud OnRamp for SaaS probe. Depending on the type of routers at the site, you can view details of the **vQoE Score** as follows: • Cisco IOS XE Catalyst SD-WAN devices: To show a chart of the vQoE score history for each available interface, click the chart icon. In the chart, each interface vQoE score history is presented as a colored line. A solid line indicates that Cloud OnRamp for SaaS has designated the interface as the best path for the cloud application at the given time on the chart. You can place the cursor over a line, at a particular time on the chart, to view details of the vQoE score of an interface at that time. From Cisco vManage Release 20.8.1, for the Office 365 application, the chart includes an option to show the vQoE score history for a specific service area, such as Exchange, Sharepoint, or Skype. For each service area, a solid line in the chart indicates the interface chosen as the best path at a given time. If you have enabled Cloud OnRamp for SaaS to use Microsoft traffic metrics for Office 365 traffic, the choice of best path takes into account the Microsoft traffic metrics. • Cisco vEdge devices: To show a chart of the vQoE score history, click the chart icon. The chart shows the vQoE score for the best path chosen by Cloud OnRamp for SaaS.
DIA Status	The type of connection to the internet, such as local (from the site), or through a gateway site.
Selected Interface	The interface providing the best path for the cloud application. **Note** If the DIA status is Gateway, this field displays **N/A**. From Cisco Catalyst SD-WAN Manager Release 20.13.1, if the best path is a loopback interface, this field displays the interface bind to the loopback.
Activated Gateway	For a site that connects to the internet through a gateway site, this indicates the IP address of the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.
Local Color	For a site that connects to the internet through a gateway site, this is the local color identifier of the tunnel used to connect to the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.

Field	Description
Remote Color	For a site that connects to the internet through a gateway site, this is the remote (gateway site) color identifier of the tunnel used to connect to the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.
SDWAN Computed Score	This field is applicable only if the site uses Cisco IOS XE Catalyst SD-WAN devices. It does not apply for Cisco vEdge devices. From Cisco vManage Release 20.8.1, for the Microsoft Office 365 application, an **SDWAN Computed Score** column provides links to view charts of the path scores (OK, NOT-OK, or INIT) provided by Microsoft telemetry for each Microsoft service area, including Exchange, Sharepoint, and Skype. The chart shows the scores over time for each available interface. The scores are defined as follows: • **OK**: Acceptable path • **NOT-OK**: Unacceptable path • **INIT**: Insufficient data These charts provide visibility into how Cloud OnRamp for SaaS chooses a best path for each type of Microsoft Office 365 traffic. A use case for viewing the path score history is for determining whether Microsoft consistently rates a particular interface as NOT-OK for some types of traffic, such as Skype traffic.

Monitor the Status of Webex for Cloud OnRamp for SaaS

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for SaaS**.

   The page displays each monitored application, the relevant sites, with information about each.

2. Optionally, you can click a site to display a chart of the scores for various available paths for the application traffic, and the best path (solid line).

3. Beginning with Cisco vManage Release 20.10.1, for each site and region, you can view information about the interfaces that Webex traffic is using. For information, see View Application Usage, on page 179.

View Server Information Using the SD-AVC Cloud Connector

Before You Begin

- Enable SD-AVC (**Administration** > **Cluster Management**, click **…** and choose **Edit**, and choose **Enable SD-AVC**).

- Enable the SD-AVC Cloud Connector. See Enable Cisco SD-AVC Cloud Connector in the *Cisco Catalyst SD-WAN Getting Started Guide*.

View Server Information

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **SD-AVC Cloud Connector**.
2. In the **Application** field, choose an application.
   - For the Office 365 application, the **SD-AVC Cloud Connector** page shows the following information collected from Microsoft Cloud about the Microsoft application servers that handle Office 365 traffic:

Field	Description
Domain tab	
Application Name	Name of the application producing the traffic. Network-Based Application Recognition (NBAR), a component of Cisco IOS XE, provides the application name.
Domain	Destination domain of the traffic. This is the application server handling the cloud application traffic.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates traffic that does not have a defined category.
Service Instance	Service instance information, as defined by Microsoft, for the server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD.
IP Address tab	
IP	Destination IP of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.
Application	Name of the application producing the traffic. NBAR, a component of Cisco IOS XE, provides the application name.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates that traffic does not have a defined category.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Service Instance	Service instance information, as defined by Microsoft, for the server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD.

- (Minimum release: Cisco vManage Release 20.10.1) For the Webex application, the **SD-AVC Cloud Connector** page shows the following information collected from Webex cloud servers:

Field	Description
IP Address tab	
Application Name	Name of the application producing the traffic.
Service Area	Type of Webex traffic: meeting, calling, or teams.
IP Address	Destination IP address of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port or ports of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.
Quality of Service	QoS classification for the Webex traffic, as defined by Webex, such as default or optimizemedia.
Primary or Fallback	Category of Webex traffic.
Region	Region of the Webex server data center, such as ap-south-1, ap-northeast-1, and ap-southeast-1.

3. Optionally, you can use the search field to filter the information in the table. For example, you can filter by an application name or by a domain name.

Monitor an Excluded Data Prefix List for Cloud OnRamp for SaaS

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click on the device to select it.
3. Click **Real Time** in the left pane.
4. Click the **Device Options** drop-drop list, and choose **Policy App Route Filter**.

A table displays real-time statistics, including the packet counter name that represents the data prefix list for an application.

View Logs in Syslog And Console Log

The Cisco Cloud OnRamp for SaaS notifications and alarms are populated in the syslog. These notifications and alarms are not populated in the console log. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the Cisco Cloud OnRamp for SaaS notifications and alarms are displayed both in syslog and console logs. However, to avoid flooding of notifications and alarms on both syslog and console logs, Cisco SD-WAN Manager generates NETCONF by default, the syslogs on demand and the console logs when you add a CLI template. For more information about using CLI templates, see CLI Add-on Feature Templates and CLI Templates.

1. Use the **system** *alarms alarm cloud-express-score change syslog* command using a CLI template to print the cloud express score change notifications both in syslogs and console logs.
2. Use the **system** *alarms alarm cloud-express-application-change syslog* command using a CLI template to print the cloud express application change notifications both in syslogs and console logs.

Cloud onRamp for SaaS Over SIG Tunnels

Table 54: Feature History

Feature Name	Release Information	Description
Cloud onRamp for SaaS Over SIG Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to connect to Cloud onRamp for SaaS by means of a SIG tunnel. The Cloud onRamp for SaaS Over SIG Tunnels feature provides you with secure access to the SaaS applications, and the capability to automatically select the best possible SIG tunnel for accessing the SaaS applications.

Prerequisites for Cloud onRamp for SaaS Over SIG Tunnels

- The SIG tunnels created using the Secure Internet Gateway (SIG) template must have a valid Tracker Source IP address. Cloud onRamp for SaaS uses the Tracker Source IP address in the SIG template for probing purposes.
- Configure the device to use an internet-based DNS server with an IP address that can be reached through the SIG tunnel.

Restrictions for Cloud OnRamp for SaaS Over SIG Tunnels

- Application identification:

  An application must be identified by Cloud OnRamp for SaaS from the very first packet in a flow going through the edge routers, between a branch and Cloud OnRamp for SaaS. If an application cannot be identified in the first packet of a flow, the best path that is selected by Cloud OnRamp cannot be implemented for the subsequent packets in that given flow. After an application is classified, the subsequent traffic flow goes through the best path selected by Cloud OnRamp for SaaS.

- Gateway exit and DIA:

  Cloud OnRamp for SaaS comparison logic between a gateway exit and a Direct Internet Access (DIA) exit cannot determine if the Cloud OnRamp for SaaS in the remote gateway is executing a computation with an underlay interface or a SIG interface.

- IPv6 support:

IPv6 is not supported with Cloud OnRamp for SaaS.

- Support for telemetry:
  - You cannot enable Microsoft 365 telemetry or Webex server-side metrics on a site that uses Cloud OnRamp for SaaS over SIG tunnels.
  - From Cisco Catalyst SD-WAN Manager Release 20.14.1, in a scenario that includes (a) sites that use Cloud OnRamp for SaaS over SIG tunnels, and also (b) sites that use Cloud OnRamp for SaaS without SIG tunnels, Microsoft 365 telemetry and Webex server-side metrics are supported only on the sites that do not use a SIG tunnel.

    When you enable Microsoft 365 telemetry or Webex server-side metrics globally, they are active only on sites that do not use Cloud OnRamp for SaaS over SIG tunnels.
  - From Cisco vManage Release 20.6.1 through Cisco Catalyst SD-WAN Manager Release 20.13.x, in a scenario that includes (a) sites that use Cloud OnRamp for SaaS over SIG tunnels, and also (b) sites that use Cloud OnRamp for SaaS without SIG tunnels, Microsoft 365 telemetry and Webex server-side metrics are not supported on any of the sites in the network.

    If you attempt to enable Microsoft 365 telemetry or Webex server-side metrics in this scenario, an error appears in the task list, associated with the push feature template configuration task.

Information About Cloud OnRamp for SaaS Over SIG Tunnels

Using Cloud OnRamp for SaaS, a site can connect to SaaS applications through the following:

- Through the best performing SIG tunnel
- Through a gateway site in which the traffic is sent through the best-performing overlay tunnel from the branch to the gateway, and then from the gateway site through the best-performing SIG tunnel.

When you configure Cloud OnRamp for SaaS for a site to connect over SIG tunnels, you have secure access to the SaaS applications over the internet.

From Cisco Catalyst SD-WAN Control Components Release 20.6.1 and Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cloud OnRamp for SaaS supports faster failover on SIG tunnels by default, if the SIG tunnels are configured with Layer 7 health check. For more information about configuring Layer 7 health check, see Support for Layer 7 Health Check.

Benefits of Cloud onRamp for SaaS Over SIG Tunnels

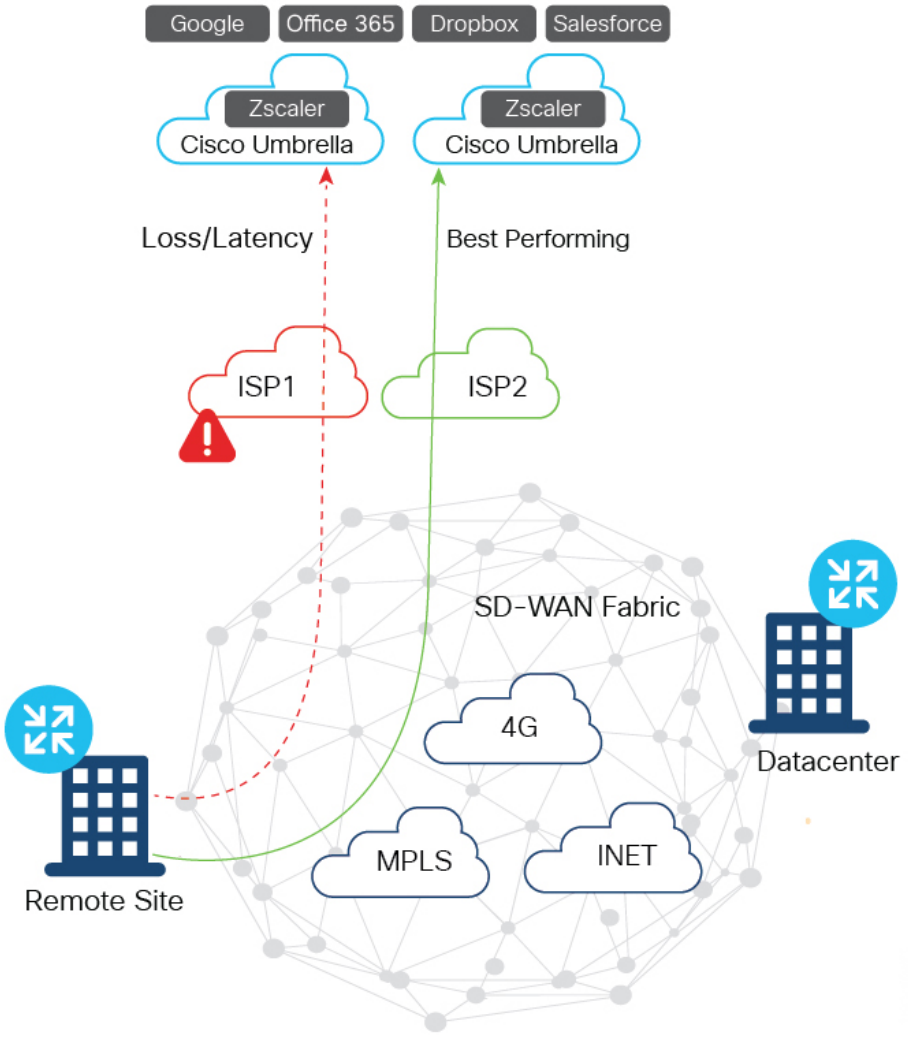
Connecting to Cloud OnRamp for SaaS over SIG tunnels has the following benefits:

- You have secure access to the SaaS applications over SIG tunnels.
- Cloud onRamp for SaaS over SIG tunnels provides best path performance where access to the SaaS applications is enabled through the best-performing tunnel.

Use Cases for Cloud onRamp for SaaS Over SIG Tunnels

There are different ways through which you can access the SaaS applications over SIG tunnels:

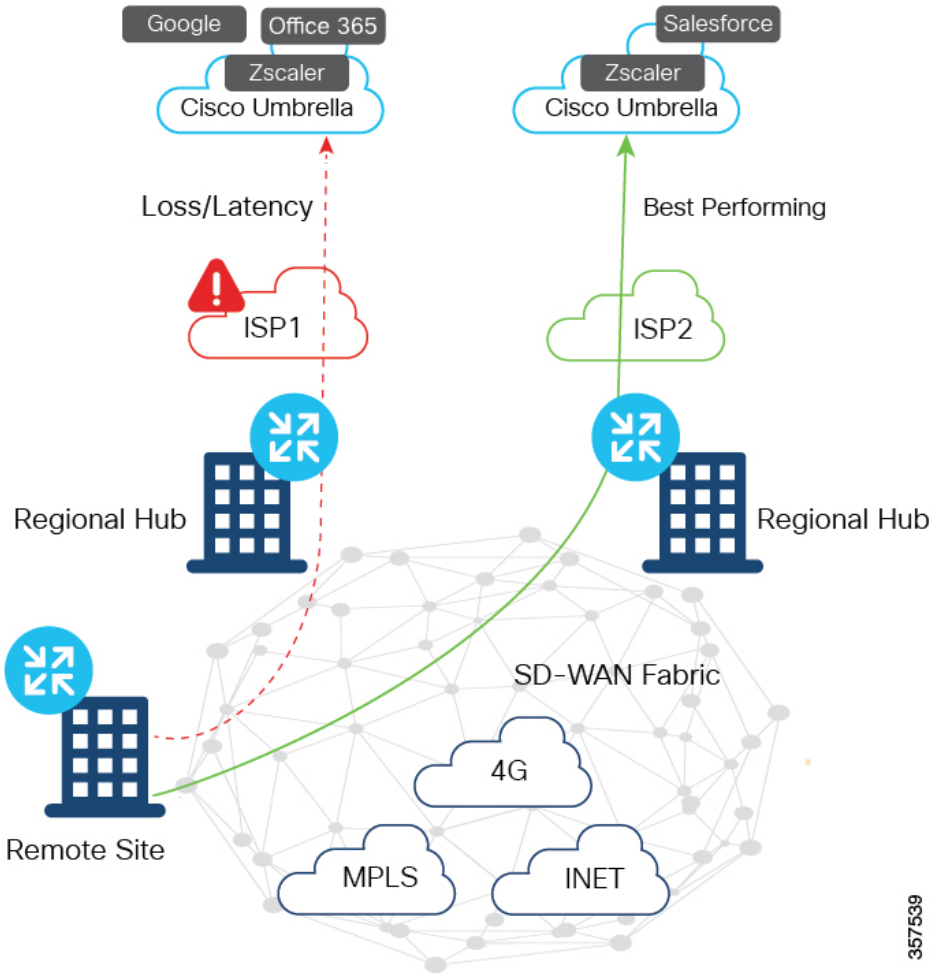
Direct Access to SaaS Applications with Multiple SIG Tunnels from Branch Using DIA



In this scenario:

- Multiple VPN0 tunnels over GRE or IPSec are set up from a branch to Zscaler and Cisco Umbrella.
- Traffic from the branch is forwarded through the best-performing tunnel for a given SaaS application, and is terminated at Zscaler and Cisco Umbrella for security inspection.
- Traffic is forwarded to the internet from SIG.

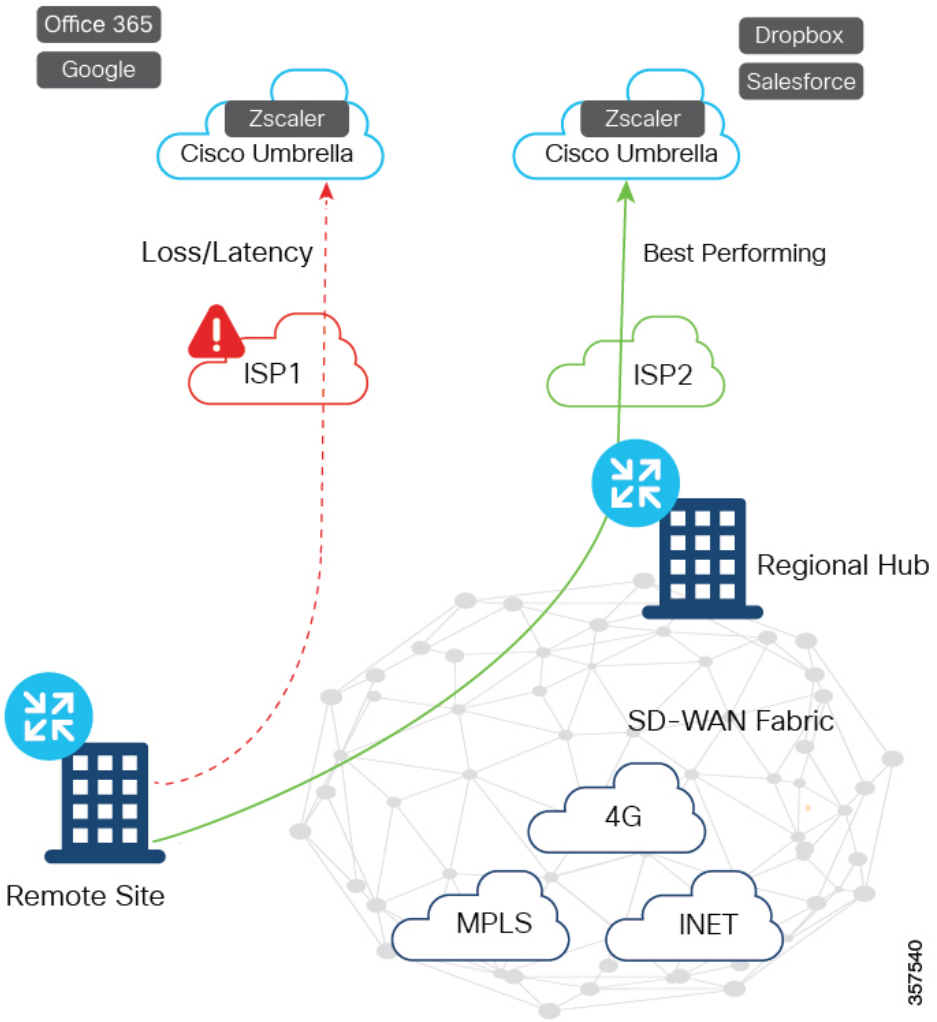
Access to SaaS Applications with Multiple SIG Tunnels from Branch Using a Gateway



In this scenario:

- Multiple VPN0 tunnels over GRE or IPSec are set up from one or more regional hubs to Zscaler and Cisco Umbrella.
- Traffic from branch is forwarded to the best-performing regional hub for a given SaaS application, and is terminated at Zscaler and Cisco Umbrella for security inspection.
- Traffic is forwarded to the internet from SIG.

Access to SaaS Applications with Multiple SIG Tunnels from Branch Using DIA and Gateway



In this scenario:

- Multiple VPN0 tunnels over GRE or IPsec are set up from a branch, regional hub, or both to Zscaler and Cisco Umbrella.
- Traffic from branch, regional hub, or both is forwarded through the best-performing tunnel for a given SaaS application, and is terminated at Zscaler and Cisco Umbrella for security inspection.
- Traffic is forwarded to the internet from SIG.

Configure Cloud OnRamp for SaaS Over SIG Tunnels

Configure Cloud OnRamp for SaaS over SIG Tunnels Using DIA

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. From **Manage Cloud OnRamp for SaaS** drop-down list, choose **Direct Internet Access (DIA) Sites**.

3. Click **Attach DIA Sites**.

   The **Attach DIA Sites** dialog box displays all the sites in your overlay network, with the available sites highlighted.

4. In **Device Class**, select:

   Cisco OS (cEdge)

5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow.

6. Click **Add TLOC to selected sites**.

7. Click **Secure Internet Gateway (SIG) Interfaces**.

8. Click **All Auto SIG Interfaces** or **SIG Interface List** from **Attach DIA Sites** window, and then choose from the list of tunnels that are configured from the Cisco Secure Internet Gateway template.

Note The Tunnel1000X entry in the **SIG Interface List** field refers to the interface name, the equivalent of the IPSec interface name entered when configuring a SIG template.

9. Click **Save Changes**.

10. Click **Attach**.

    Cisco SD-WAN Manager pushes the feature template configuration to the devices, and the **Task View** window displays a `Validation Success` message.

Configure Cloud OnRamp for SaaS over SIG Tunnels Using a Gateway

To configure Cloud OnRamp for SaaS over SIG tunnels a Gateway, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

2. From **Manage Cloud OnRamp for SaaS** drop-down list, choose **Gateways**.

3. Click **Attach Gateways**.

   The **Attach Gateways** pop-up window displays all the sites in your overlay network, with available sites highlighted.

4. In **Device Class**, select:

   Cisco OS (cEdge)

5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow

6. Click **Add interfaces to selected sites**.

7. Click **VPN 0**.

8. Click **Secure Internet Gateway (SIG) Interfaces**.

9. Click **All Auto SIG Interfaces**, or **SIG Interface List** from **Attach Gateways** window, and then choose from the list of tunnels that are configured from the Cisco Secure Internet Gateway template.

Note The Tunnel1000X entry in the **SIG Interface List** field refers to the interface name, the equivalent of the IPSec interface name entered when configuring a SIG template.

10. Click **Save Changes**.
11. Click **Attach**. Cisco SD-WAN Manager pushes the feature template configuration to the devices, and the **Task View** window displays a **Validation Success** message.

Configure Cloud onRamp for SaaS Over SIG Tunnels Using the CLI

This section provides sample CLI configurations for Cloud onRamp for SaaS over SIG tunnels.

Configure Cloud OnRamp for SaaS over SIG Tunnels for DIA and Gateway Sites

```
Device# config-transaction
Device(config)# probe-path {branch|gateway}
{all-auto-sig-tunnels|sig-tunnel-list} list of SIG tunnels
Device(config)# ip sdwan route vrf vrf ip address service sig
```

Enable NBAR Protocol Discovery for Cloud OnRamp for SaaS Over SIG Tunnels for Gateway Sites

```
Device# config-transaction
Device(config)# probe-path gateway {all-auto-sig-tunnels|sig-tunnel-list} list
 of SIG tunnels
Device(config)# ip sdwan route vrf vrf ip address service sig
Device(config)# interface tunnel-id
Device(config-if)# ip nbar protocol-discovery
```

Example

The following example configures Cloud onRamp for SaaS over SIG tunnels for a gateway site and enables NBAR protocol discovery on tunnel interfaces Tunnel100001 and Tunnel100002.

```
Device# config-transaction
Device(config)# probe-path gateway all-auto-sig-tunnels
Device(config)# ip sdwan route vrf 1 192.168.0.1 service sig
Device(config)# interface Tunnel101
Device(config-if)# ip nbar protocol-discovery
Device(config-if)# interface Tunnel102
Device(config-if)# ip nbar protocol-discovery
```

Configure VPN with Loopback Interfaces

```
Device# config-transaction
Device(config)# vrf definition vrf
Device(config-vrf)# address-family ipv4
Device(config-vrf)# exit-address-family

Device(config)# interface  Loopback interface_number
Device(config-if)# no shutdown
```

```
Device(config-vrf)# vrf forwarding vrf_number
Device(config-vrf)# ip address ip address mask
Device(config-vrf)# exit
```

Monitor Cloud OnRamp for SaaS Over SIG Tunnels

To monitor Cloud OnRamp for SaaS over SIG tunnels, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. From the list of devices that is displayed, select a device.
3. Click **Real Time** in the left pane.
4. Click **Device Options** drop-drop list, and choose one of the following commands:

Device Option	Description
CloudExpress Applications	Displays the best path for applications that are configured with Cloud OnRamp for SaaS. The best path could be a local interface with DIA, or the path to a remote gateway.
CloudExpress Gateway Exits	Displays the loss and latency on each gateway exit for applications that are configured with Cloud OnRamp for SaaS.
CloudExpress Local Exits	Displays the application loss and latency on each DIA interface that is enabled for Cloud OnRamp for SaaS.

5. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud onRamp for SaaS** to access the dashboard where you can view the applications available on Cloud OnRamp for SaaS.

Monitor Cloud onRamp for SaaS Over SIG Tunnels Using the CLI

Example 1

The following is a sample output from the **show sdwan cloudexpress local-exits** command on Cisco IOS XE Catalyst SD-WAN devices . This example displays the application loss and latency on each DIA interface that is enabled for Cloud OnRamp for SaaS.

```
Device# show sdwan cloudexpress local-exits

VPN APPLICATION INTERFACE LATENCY LOSS
------------------------------------------------------------------------
1 office365 Tunnel100015 10 0
1 office365 Tunnel100016 3 0
1 amazon_aws Tunnel100015 10 0
1 amazon_aws Tunnel100016 3 0
```

Example 2

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the loss and latency on each gateway exit for applications that are configured with Cloud OnRamp for SaaS.

```
Device# show sdwan cloudexpress gateway-exits

                                                                                LOCAL  REMOTE
VPN  APPLICATION              GATEWAY IP               LATENCY  LOSS  COLOR  COLOR
-------------------------------------------------------------------------------------------
1    salesforce               172.16.255.14            72       2     lte    lte
1    google_apps              172.16.255.14            16       0     lte    lte
```

Example 3

The following is a sample output from the **show sdwan cloudexpress applications** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the best path for applications that are configured with Cloud OnRamp for SaaS. The best path could be a local interface with DIA, or the path to a remote gateway.

```
Device# show sdwan cloudexpress applications

                                EXIT     GATEWAY
LOCAL  REMOTE
VPN  APPLICATION                TYPE     SYSTEM IP      INTERFACE  LATENCY  LOSS
COLOR  COLOR
-----------------------------------------------------------------------------------------------
1    salesforce                 gateway  172.16.255.14  -          103      1
lte    lte
1    google_apps                gateway  172.16.255.14  -          47       0
lte    lte
```

Example 4

The following is a sample output from the **show ip route vrf** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the IP routing table that is associated with a specific VPN routing and forwarding (VRF) instance.

```
Device# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

Example 5

The following is a sample output from the **show sdwan run probe-path** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the probe path for SIG tunnels.

```
Device# show sdwan run probe-path
probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
```

Configuration Example for Cloud onRamp for SaaS Over SIG Tunnels

The following example shows the configuration of Cloud on Ramp for SaaS over SIG tunnels:

Example

```
Device(config)# probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
Device(config)# probe-path branch all-auto-sig-tunnels
```

Troubleshooting Cloud OnRamp for SaaS

The following sections describe problem scenarios and troubleshooting information.

Cannot Enable Telemetry for the Webex Application

Problem

You cannot enable telemetry for the Webex application in Cloud OnRamp for SaaS.

Solutions

For context for each of the following steps, see Enable Webex Server-Side Metrics, on page 174.

1. Ensure that you have created the application integration, using the Webex developer site.
2. Ensure that you have entered the correct redirect URL, in the format below:

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect
3. Ensure that when you enable Webex in Cloud OnRamp for SaaS, you enter the correct client ID and client secret.

Failing to Identify the Best Path for Each Webex Region

Problem

Cloud OnRamp for SaaS fails to identify the best path for each Webex region.

Solutions

1. If a device fails to identify the best path, run the **show avc sd-service info connectivity** command on the device to ensure that Cisco SD-AVC is enabled.
2. From the Cisco SD-WAN Manager menu, choose **Monitor** > **SD-AVC Cloud Connector**. Choose the **Webex** application and verify that the region field is populated.

3. Verify that DNS and NAT are operating correctly, outside of the context of Cloud OnRamp for SaaS configuration. Cloud OnRamp for SaaS functionality depends on these to be configured correctly.
4. Verify that the region's responder server is operational and reachable by the device. To do this, ping the server from the device and verify that the server responds to the ping.

   The regional responder server names are in the following format:

   pinger.*region-name*.infnet.webex.com

   The following example is for the us-west region:

   ```
   Device#ping pinger.us-west-1.infnet.webex.com
   ```

Debug and Show Commands

Note The following debug and show commands are applicable for Cisco IOS XE Catalyst SD-WAN devices running Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and later.

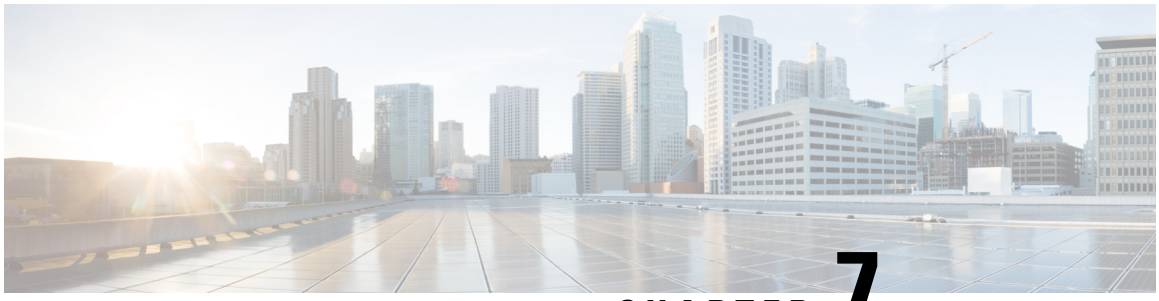
Table 55:

Description	Command
To debug the CXP and Cisco SD-WAN Analytics interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-analytics* **debug**
To analyze the verbose level debug traces of the CXP and Cisco SD-WAN Analytics interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-analytics* **verbose**
To set platform software trace cxpd RP active cxpd-analytics notice to set the debug level to the notice level debug traces of CXP and Cisco SD-WAN Analytics interaction scenarios (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-analytics* **notice**
To enable debug traces to analyze the CXP App best path selection logic handling	Use the command **set platform software trace** *cxpd RP active cxpd-app* **debug**
To enable verbose level debug traces to analyze the CXP App best path selection logic handling	Use the command **set platform software trace** *cxpd RP active cxpd-app* **verbose**
To set the debug level to the notice level and to disable the CXP App best path selection logic handling debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-app* **notice**
To enable debug traces to analyze the CXP config parsing handling	Use the command **set platform software trace** *cxpd RP active cxpd-config* **debug**
To enable debug traces to analyze the verbose level CXP config parsing handling	Use the command **set platform software trace** *cxpd RP active cxpd-config* **verbose**

Description	Command
To set the debug level to the notice level and to disable the CXP config parsing handling debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-config* **notice**
To enable debug traces to analyze the CXP and DPI module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-dpi* **debug**
To enable verbose level debug traces to analyze the CXP and DPI module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-dpi* **verbose**
To set the debug level to the notice level and to disable the CXP and DPI module interaction scenarios debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-dpi* **notice**
To debug traces to analyze the CXP and FTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ftm* **debug** This trace can be enabled to analyze the data plane programming issues from CXP. From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the *cxpd-ftm* keyword in this command is deprecated
To debug traces to analyze the CXP and FMANRP module interaction scenarios	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, use the command **set platform software trace** *cxpd RP active cxpd-fmanrp* **debug** This trace can be enabled to analyze the data plane programming issues from CXP.
To enable verbose level debug traces to analyze the CXP and FTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ftm* **verbose** From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, *cxpd-ftm* keyword in this command is deprecated.
To enable verbose level debug traces to analyze the CXP and FMANRP module interaction scenarios	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, use the command **set platform software trace** *cxpd RP active cxpd-fmanrp* **verbose**
To set the debug level to the notice level and to disable the CXP and FTM module interaction scenarios debugs enabled (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-ftm* **notice** From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the *cxpd-ftm* keyword in this command is deprecated.
To set the debug level to the notice level and to disable the CXP and FMANRP module interaction scenarios debugs enabled (this disables all the trace levels higher than notice)	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, use the command **set platform software trace** *cxpd RP active cxpd-fmanrp* **notice**

Description	Command
To enable debug traces to analyze the CXP and OMP module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-omp* **debug** This trace can be enabled to analyze the CXP Gateway metrics handling issues
To enable verbose level debug traces to analyze the CXP and OMP module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-omp* **verbose**
To set the debug level to the notice level and to disable the CXP and OMP module interaction scenario debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-omp* **notice**
To enable debug traces to analyze the CXP operational commands handling	Use the command **set platform software trace** *cxpd RP active cxpd-oper* **debug**
To enable verbose level debug traces to analyze the CXP operational commands handling	Use the command **set platform software trace** *cxpd RP active cxpd-oper* **verbose**
To set the debug level to the notice level and to disable the CXP operational parsing handling debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-oper* **notice**
To enable debug traces to analyze the CXP and IOS interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-rtm* **debug**
To enable verbose level debug traces to analyze the CXP and IOS module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-rtm* **verbose**
To set the debug level to the notice level and to disable the CXP probe metrics debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-rtm* **notice**
To enable debug traces to analyze the CXP probe metrics handling issues	Use the command **set platform software trace** *cxpd RP active cxpd-telemetry* **debug**
To enable verbose level debug traces to analyze the CXP probe metrics handling issues	Use the command **set platform software trace** *cxpd RP active cxpd-telemetry* **verbose**
To set the debug level to the notice level and to disable the CXP probe metrics debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-telemetry* **notice** level
To enable debug traces to analyze the CXP and TTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ttm* **debug**
To enable verbose level debug traces to analyze the CXP and TTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ttm* **verbose**
To set the debug level to the notice level and to disable the CXP and TTM module interaction scenarios debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-ttm* **notice**

Description	Command
To enable debug traces to analyze the CXP module level issues (mostly during the bootup scenarios)	Use the command **set platform software trace** *cxpd RP active cxpd-misc* **debug**
To enable debug traces to analyze the verbose CXP module level issues (mostly during the bootup scenarios)	Use the command **set platform software trace** *cxpd RP active cxpd-misc* **verbose**
To set the debug level to the notice level and to disable the CXP module level debugs and (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-misc* **notice**
To check the trace levels of different CXPD btraces enabled	Use the command **show platform software trace** *level cxpd* **RP active**
To view syslogs and console logs	Use the command **show** *sdwan notification stream viptela*



CHAPTER 7

Application Lists

Table 56: Feature History

Feature Name	Release Information	Description
User-Defined SaaS Application Lists	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature expands the range of SaaS applications that Cloud OnRamp for SaaS can monitor, and for which it can determine the best network path. The feature enables you to define lists of one or more SaaS applications, together with the relevant application server for those SaaS applications. Cloud OnRamp for SaaS handles these lists in the same way that it handles the predefined set of SaaS applications that it can monitor. When you enable a user-defined list, Cloud OnRamp for SaaS probes for the best path to the application server and routes the application traffic for applications in the list to use the best path.

- Information About SaaS Application Lists, on page 201
- Prerequisites for SaaS Application Lists, on page 203
- Restrictions for SaaS Application Lists, on page 203
- Use Cases for SaaS Application Lists, on page 203
- Workflow, on page 205
- Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager, on page 205
- View SaaS Application Lists, on page 206

Information About SaaS Application Lists

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

SaaS Application Lists

Cisco SD-WAN Manager provides a preset list of several cloud applications that Cloud OnRamp for SaaS can monitor to determine the best path for the cloud application traffic, including Amazon AWS, Box, and so on. Although Cisco SD-WAN Manager presents each of these as a singular cloud application, the cloud application is, in fact, a list that may include a set of closely related applications, but the details do not appear in Cisco SD-WAN Manager. For example, the Amazon AWS option includes a list of multiple applications

that all contribute to the application traffic for Amazon AWS functionality. This is called a SaaS application list.

For each SaaS application list, Cloud OnRamp for SaaS probes a single application server, called the probe endpoint, to determine the best path for network traffic for the applications in the list.

NBAR

Each of the cloud applications in a SaaS application list is an application as defined by Cisco network based application recognition (NBAR), a technology that identifies network traffic according to the network application that produced the traffic. Based on the installed Protocol Pack, NBAR operates with a standard set of applications that it can identify (see Protocol Pack). In addition to the standard set of applications, you can define custom applications (see Define Custom Applications) to extend the scope of applications that NBAR can identify.

User-Defined SaaS Application Lists

You can create a user-defined SaaS application list that includes one or more related applications. The applications can be standard applications that NBAR identifies using the installed Protocol Pack, or custom applications.

For each SaaS application list, you specify an application server as the probe endpoint. Cloud OnRamp for SaaS probes this server to determine the best path to use for traffic produced by the applications in the SaaS application list.

Cloud OnRamp for SaaS handles user-defined SaaS application lists in the same way that it handles the predefined set of SaaS applications that it can monitor. When you enable a user-defined list, Cloud OnRamp for SaaS probes for the best path to the application server and routes the application traffic for applications in the list to use the best path.

Note When an application with an existing endpoint is split or updated due to a protocol pack update, the app doesn't inherit the predefined endpoint from the parent app.

You should update the endpoint manually for such an app.

Note In contrast to user-defined custom applications, user-defined SaaS application lists do not appear as an option for matching when creating policies. (See the Cisco SD-WAN Policies Configuration Guide.)

Benefits of SaaS Application Lists

User-defined SaaS application lists expand the scope of Cloud onRamp for SaaS to include additional cloud applications. Application lists extend the benefits of Cloud onRamp for SaaS to cloud applications of specific interest to an organization.

Prerequisites for SaaS Application Lists

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

- SD-AVC is enabled.
- A centralized policy is defined and active.

  For information about defining a centralized policy, see the Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x.
- If a gateway site uses a SIG tunnel as its direct internet access (DIA) connection, then in the configuration of the tunnel, enable NBAR protocol discovery.

  For information about enabling NBAR protocol discovery, see Configure Cloud onRamp for SaaS Over SIG Tunnels Using the CLI, on page 193.

Restrictions for SaaS Application Lists

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

- A SaaS application list can include only up to eight applications. The recommended custom application lists that can be enabled for monitoring and policy on Cisco SD-WAN Manager is eight. The Cisco IOS XE Catalyst SD-WAN devices have a limitation to support only 32 custom applications due to a policy limitation.
- A SaaS application list under each data-policy on each sequence should not exceed 32.
- Username and password with special characters in SaaS custom application endpoint-url is not allowed.
- Starting Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, new checks to restrict the invalid URLs are added. If there is an invalid URL defined with the Cisco IOS XE Catalyst SD-WAN device prior to Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, then when you upgrade to Cisco IOS XE Catalyst SD-WAN Release 17.15.1a or later, the URL will be rejected when you try to edit the URL.

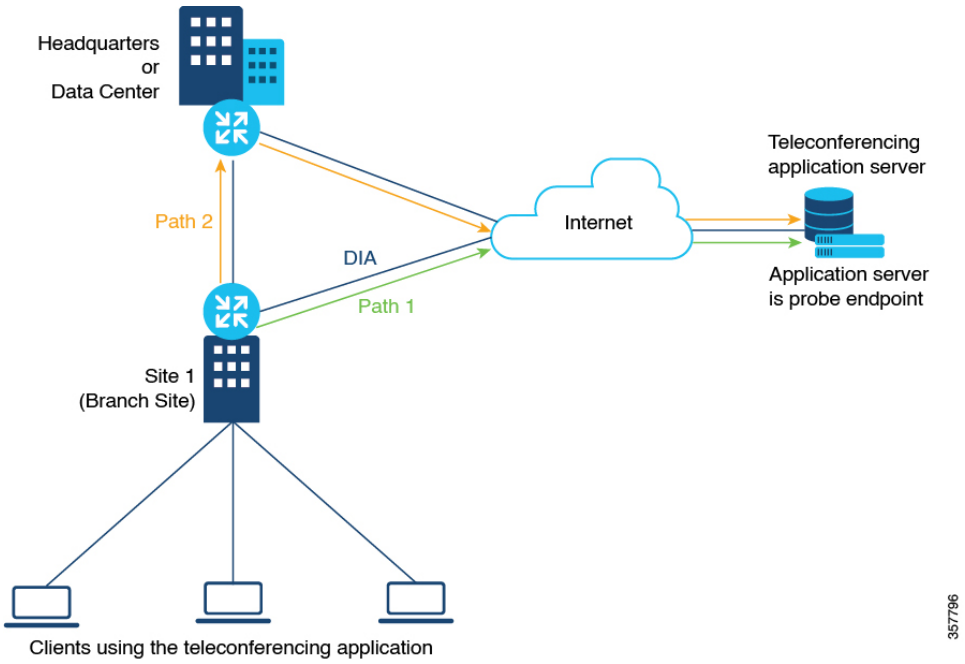
Use Cases for SaaS Application Lists

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

Scenario

An organization uses an uncommon teleconferencing system that is not recognized by NBAR. The teleconferencing system uses three different network applications to manage audio, video, and other media traffic. All three applications connect to a front-end application server at the following domain within the organization: teleconf-internal.example.com

Figure 19: Use Case



Custom Applications

To track network traffic produced by the teleconferencing system, a network administrator defines three custom applications using the server name described above or L3/L4 traffic attributes (see Define Custom Applications) to identify traffic from the three applications, as follows:

- teleconf-system-audio
- teleconf-system-video
- teleconf-system-media

With these custom applications defined, NBAR can identify traffic from each of the three applications.

SaaS Application List

To optimize the best path for the set of three teleconferencing-related network applications, a network administrator creates a SaaS application list called teleconf-system, and adds each of the three related custom applications to this application list.

SaaS application list: teleconf-system
Applications in the list: teleconf-system-audio, teleconf-system-video, teleconf-system-media

For the probe endpoint for the SaaS application list, the network administrator specifies the front-end server described above (teleconf-internal.example.com), which handles traffic for the three applications.

The result is an application list, teleconf-system, which includes the three applications. The network administrator enables the teleconf-system application list in Cloud onRamp for SaaS, and Cloud onRamp for SaaS begins probing for the best path to the front-end server. Cloud onRamp for SaaS routes the traffic for these three applications to the best path for the front-end server.

Workflow

1. If you choose to include custom applications (for applications not included in the Protocol Pack) in an application list, define the custom applications using the procedure described in Define Custom Applications.
2. Create an application list with one or more applications.

   See Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager, on page 205.
3. Enable the application list in Cloud OnRamp for SaaS.

   See Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager.

Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. Open the Cloud OnRamp for SaaS page, using one of the following methods:
   - From the Cisco SD-WAN Manager main menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     or
   - From the Cisco SD-WAN Manager menu, click the cloud icon near the top right and select **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **SaaS Application Lists**.
3. Click **New Custom Application List**.
4. Enter a name for the list.
5. To add applications to the list, click the **Search** field and choose applications. The list includes standard applications and any custom applications that you have defined.

   Optionally, you can enter text in the **Search** field to filter for specific applications.

   The applications that you choose are added to the **Application** field, which shows each application in the list.
6. Optionally, to create a new custom application within this workflow, click the **Search** field and then click **New Custom Application**. Creating a custom application on this page is equivalent to defining a custom application in the centralized policy workflow, as described in Define Custom Applications. See Define Custom Applications Using Cisco SD-WAN Manager for information about the what information is required for defining a custom application, the use of wildcard characters, the logic applied when matching traffic to the attributes that you enter, and so on.
7. In the **SaaS Probe Endpoint Type** area, define the probe endpoint, which is the server that Cloud OnRamp for SaaS probes to determine a best path for the traffic in the SaaS application list.

- Choose an endpoint type from the following options:
  - **IP Address**: Enter an IP address. Cloud OnRamp for SaaS probes the server using port 80.
  - **FQDN**: Enter a fully qualified domain name.
  - **URL**: Enter a URL using HTTP or HTTPS. Cloud OnRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.
- Enter an endpoint value, based on the endpoint type that you choose.

  Examples: 192.168.0.1, https://www.example.com

8. Click **Add**. The new SaaS application list appears in the table of application lists.

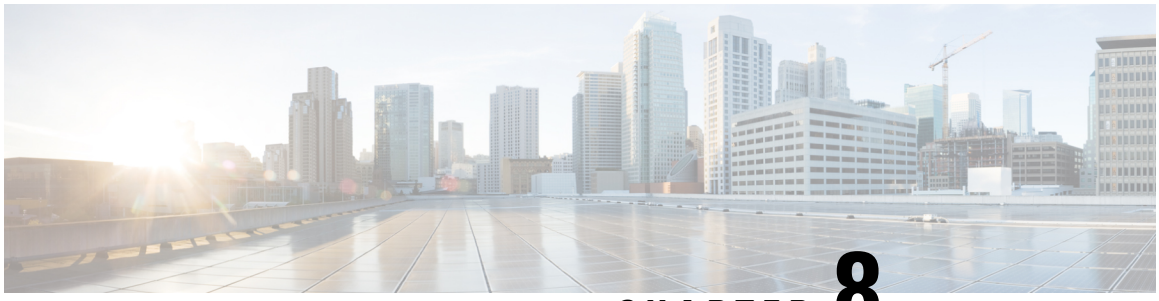
View SaaS Application Lists

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, Cisco vManage Release 20.8.1

1. Open the Cloud onRamp for SaaS page, using one of the following methods:
   - From the Cisco SD-WAN Manager main menu, choose **Configuration** > **Cloud onRamp for SaaS**.

     or
   - From the Cisco SD-WAN Manager menu, click the cloud icon near the top right and select **Cloud onRamp for SaaS**.
2. In the **Manage Cloud onRamp for SaaS** drop-down list, choose **SaaS Application Lists**.

   A table shows the details of each SaaS application list. Optionally, you can click an icon in the **Action** column to edit or delete a list.



CHAPTER 8

Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

Note Use the workflow described in this section only for devices using Cisco IOS XE Catalyst SD-WAN Release 17.2.1r. For later releases, see other sections of this guide.

This feature was released as a fully functional beta in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, with a provisioning workflow subject to change in future releases. This workflow was deprecated in Cisco IOS XE Catalyst SD-WAN Release 17.3.1a and replaced by a unified workflow that addresses Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

Table 57: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Cloud OnRamp for SaaS is available for Cisco IOS XE Catalyst SD-WAN devices, with a configuration workflow that is entirely different from the workflow that applies to Cisco vEdge devices. This feature is released as a fully functional beta in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r. The provisioning workflow is subject to change in future releases.

Many organizations rely on software-as-a-service (SaaS) applications for business-critical functions. These cloud-based services include Office365, Salesforce, Box, and many others. As cloud-based services, these SaaS applications must communicate with their own remote servers, which are available through internet connections.

At remote sites, SaaS applications may these pose special challenges:

- **Performance**: If remote sites, such as branch offices, route SaaS traffic through a centralized location, such as a data center, performance degrades, with latency that affects the user experience.
- **Inability to optimize routing**: Network administrators may not have any visibility into the performance of these SaaS applications, or any ability to change the routing of the SaaS traffic to more efficient paths.

Cloud OnRamp for SaaS (formerly called CloudExpress service) addresses these challenges. It enables you to select specific SaaS applications and interfaces, and to let SD-WAN determine the best performing path for each SaaS application, using the specified interfaces. For example, you can enable:

- routing through a direct internet access (DIA) connection at a branch site, if available
- routing through a gateway location, such as a regional data center

SD-WAN monitors each available path for each SaaS application continually, so if a problem occurs in one path, it can adjust dynamically and move SaaS traffic to a better path.

For more information, see SD-WAN: Cloud OnRamp for SaaS Deployment Guide.

- Overview: How to Configure Cloud onRamp for SaaS, on page 208
- Common Scenarios for Using Cloud onRamp for SaaS, on page 209
- Create a Probes Feature Template, on page 214
- Create a Policy for Cloud onRamp for SaaS, on page 217

Overview: How to Configure Cloud onRamp for SaaS

In contrast to using Cloud onRamp for SaaS with vEdge devices, configuring the feature for Cisco XE SD-WAN devices includes two steps:

- determining the best paths (configured by feature template)
- using the best paths (configured by policy)

Here is a high level overview of the tasks.

	Task	Component	Summary
1	Determine the best paths for SaaS applications	Feature template	Create a feature template to configure Cloud onRamp for SaaS to probe paths for specific SaaS application servers, determine the best path for each, and create a table based on these paths. SD-WAN probes periodically and updates the table with the most up-to-date information about the best path. If the topology includes gateway and branch sites, separate feature templates are required for branch sites and gateway sites. See Create a Probes Feature Template. **Note** The probes feature template is not supported for releases later than Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

	Task	Component	Summary
2	Use the best paths for SaaS applications	Policy	Create a policy to direct specific SaaS applications to use the best paths, as determined by the previous step. **Note** In the policy, specify only SaaS applications that are included in the feature template. If the policy specifies a SaaS application that is not included in the feature template, the traffic for that application uses the default path, as if Cloud onRamp for SaaS is not enabled. See "Create a Policy for Cloud onRamp for SaaS".

Common Scenarios for Using Cloud onRamp for SaaS

For an organization using SD-WAN, a branch site typically routes SaaS application traffic by default over SD-WAN overlay links to a data center. From the data center, the SaaS traffic reaches the SaaS server.

For example, in a large organization with a central data center and branch sites, employees might use Office 365 at a branch site. By default, the Office 365 traffic at a branch site would be routed over SD-WAN overlay links to a centralized data center, and from there to the Office 365 cloud server.

Scenario 1: If the branch site has a direct internet access (DIA) connection, you may choose to improve performance by routing the SaaS traffic through that direct route, bypassing the data center.

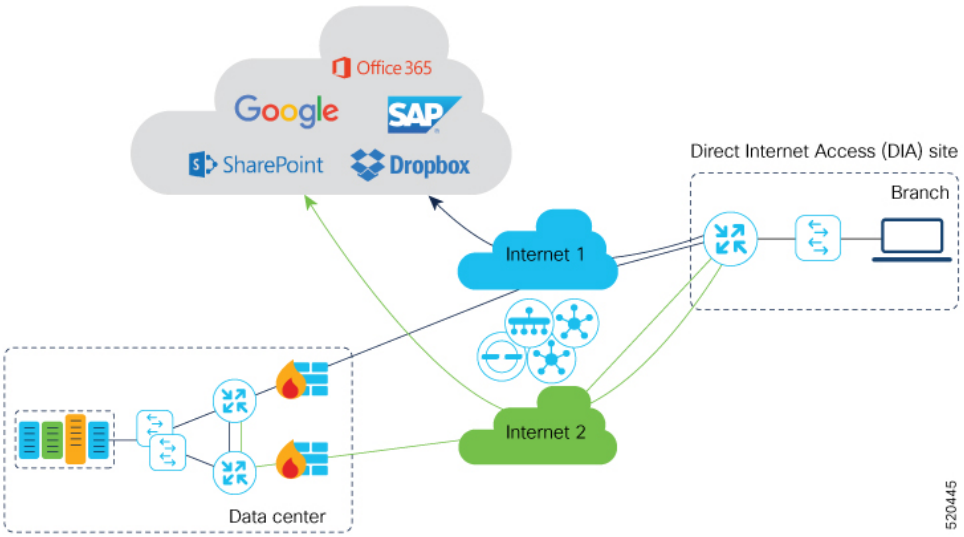
Scenario 2: If the branch site connects to a gateway site that has DIA links, you may choose to enable SaaS traffic to use the DIA of the gateway site.

Scenario 3: Hybrid method.

Scenario 1: Cloud Access through Direct Internet Access Links

In this scenario, a branch site has one or more direct internet access (DIA) links, as shown in the illustration below.

Using Cloud onRamp for SaaS, SD-WAN can select the best connection for each SaaS application through the DIA links or through the SD-WAN overlay links. Note that the best connection may differ for different SaaS applications. For example, Office365 traffic may be faster through one link, and Dropbox traffic may be faster through a different link.



Configuration Workflow

Create Probes feature template(s) only for branch sites, and configure a policy to use Cloud onRamp for SaaS.

	Task	Details
Branch sites		

1	Create a Probes feature template for branch sites.	In the Probes feature template, set parameters as follows:
		• **SaaS Mode**: SaaS Branch
		• **TLOCS** : Select either **All DIA TLOC** or **TLOC List** and select the TLOC colors in the drop-down menu.
		  • **All DIA TLOC**: Select this option if DIA is enabled for all TLOCs at a branch.
		  • **TLOC List**: If DIA is enabled only on a subset of TLOCs at a site, you can select this option and then select colors corresponding to the TLOCs that have DIA enabled.
		• **SaaS applications**: Specify applications for Cloud onRamp for SaaS.
		
		See Create a Probes Feature Template.

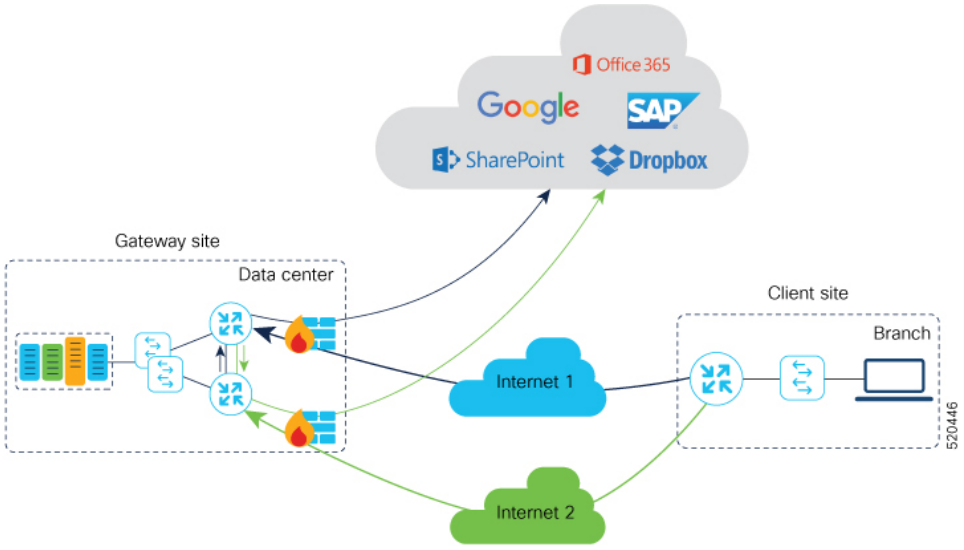
2	Use the feature template in a device template for branch sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
3	Apply the device template to branch sites.	

	Task	Details
Policy		
4	Create a policy.	In the App Route Policy, under match conditions, select the Cloud SaaS application, and specify the same applications that you specified while creating the feature template. Select the action to be Cloud SLA. See “Create a Policy for Cloud onRamp for SaaS”.
5	Activate the policy	Apply the policy to those branch sites to which the feature template created earlier was applied.

Scenario 2: Cloud Access through a Gateway Site

In this scenario, a branch site has one or more direct connections to a gateway site, and the gateway site has links to the internet.

Using Cloud onRamp for SaaS, SD-WAN can select the best connection for each SaaS application through the gateway site. If the branch site connects to more than one gateway site, SD-WAN ensures that SaaS traffic uses the best path for each SaaS application, even through different gateway sites.



Configuration Workflow

Create Probes feature template(s) for branch sites and for gateway sites, and configure a policy to use Cloud onRamp for SaaS.

	Task	Details
Branch sites		

	Task	Details
1	Create a Probes feature template for branch sites.	In the Probes feature template, set parameters as follows: • **SaaS Mode**: SaaS Branch • **TLOCS**: All DIA TLOC • **SaaS applications**: Do NOT specify any applications. **Note** Note this difference in this workflow, compared with scenario 1 (Cloud Access through Direct Internet Access Links). In this workflow, specify applications in the gateway site configuration (see below). See Create a Probes Feature Template.
2	Use the feature template in a device template for branch sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
3	Apply the device template to branch sites.	
Gateway Sites		
4	Create a Probes feature template(s) for gateway sites.	• Unless the gateway sites use identical routers and interfaces, each gateway site requires a separate feature template. • **SaaS Mode**: SaaS Gateway After selecting **SaaS Gateway**, provide the interface name on which the Probe will be initiated. This interface must be bound to a non-zero VPN. • **SaaS applications**: Specify applications for Cloud onRamp for SaaS. See Create a Probes Feature Template.
5	Use the feature template created in the previous step in a device template for gateway sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
6	Apply the device template to gateway sites.	
Policy		
7	Create a policy.	Specify the same applications as in the feature template in task 4 above. See “Create a Policy for Cloud onRamp for SaaS”.

	Task	Details
8	Activate the policy.	Apply the policy to those branch and gateway sites to which the feature templates created earlier were applied.

Scenario 3: Hybrid Approach

In this scenario, a branch site has both direct internet access (DIA) links, and links to a gateway site, which also has links to the internet.

Using Cloud onRamp for SaaS, SD-WAN can select the best connection for each SaaS application, either through DIA links or through the gateway site.

Configuration Workflow

Create Probes feature template(s) for branch sites and for gateway sites, and configure a policy to use Cloud onRamp for SaaS.

	Task	Details
Branch sites		

1	Create a Probes feature template for branch sites.	In the Probes feature template, set parameters as follows:
		• **SaaS Mode**: SaaS Branch
		• **TLOCS** : Select either **All DIA TLOC** or **TLOC List** and select the TLOC colors in the dropdown menu.
		  • **All DIA TLOC**: You can select this option if DIA is enabled for all TLOCs at a branch.
		  • **TLOC List**: If DIA is enabled only on a subset of TLOCs at a site, you can select this option and then select colors corresponding to the TLOCs that have DIA enabled.
		• **SaaS applications**: Specify applications.
		See Create a Probes Feature Template.

2	Use the feature template in a device template for branch sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
3	Apply the device template to branch sites.	
Gateway Sites		

	Task	Details
4	Create a Probes feature template(s) for gateway sites.	• Each gateway site requires a separate feature template unless the gateway sites use identical routers and interfaces. • **SaaS Mode**: SaaS Gateway After selecting **SaaS Gateway**, provide the interface name on which the Probe will be initiated. This interface must be bound to a non-zero VPN. • **SaaS applications**: Specify applications for Cloud onRamp for SaaS. See Create a Probes Feature Template.
5	Use the feature template created in the previous step in a device template for gateway sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
6	Apply the device template to gateway sites.	
Policy		
7	Create a policy.	Specify the same applications as in the feature template in task 4 above. See “Create a Policy for Cloud onRamp for SaaS”.
8	Activate the policy.	Apply the policy to those branch and gateway sites to which the feature templates created earlier were applied.

Create a Probes Feature Template

Note The probes feature template is not supported for releases later than Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

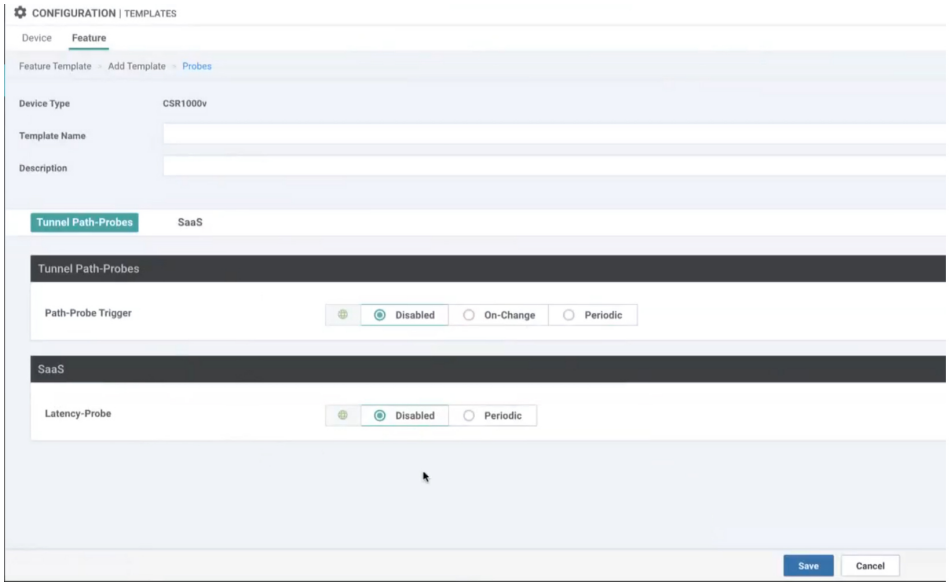
Follow these steps to create a Probes template to use Cloud OnRamp for SaaS on Cisco XE SD-WAN devices.

Create a feature template to apply either to branch site(s) or to gateway site(s). The SaaS Mode option in the template determines whether the template is for use with branch or gateway sites.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device model.
5. In **Other Templates**, click **Probes** to create a probes template for Cloud OnRamp for SaaS.



6. Configure the following fields, as desired. Choosing some of the options changes the options available in other fields.

Field	Description
Tunnel Path-Probes	
Path-Probe Trigger	Must be set to **Disabled**. **Note** Not supported in this release.
Latency-Probe	**Disabled**: Disable Cloud OnRamp for SaaS in this feature template. **Periodic**: Enable Cloud OnRamp for SaaS.
Latency-Probe Frequency	Frequency (seconds) for probing the links between the site(s) and the SaaS application cloud server(s). The probe determines latency on each available path. Range: 0 to 65535 Default: 30 **Note** Recommended: Default value of 30

Field	Description
SaaS Mode	Select the type of site for this feature template. **SaaS Branch**: For a feature template that applies to a branch site. **SaaS Gateway**: For a feature template that applies to a gateway site.
TLOCS	(Available for the SaaS Branch option of SaaS Mode) **All DIA TLOC**: Include all direct internet access (DIA) interfaces at the site that have been assigned a valid color. **TLOC List**: Indicate interfaces to include by specifying one or more colors. These interfaces determine the possible routing paths for the SaaS traffic.
TLOCS List Color	(Available for the TLOC List option of TLOCS) Use the drop-down list to select a color. You can choose multiple colors.
Interface [x]	(Available for the SaaS Gateway option of SaaS Mode) Provide one or more interface names at the gateway site. The feature template applies only to these interfaces. Example: gig2/0
Path-Probe	Must be set to **Disabled**. **Note** Not supported in this release.

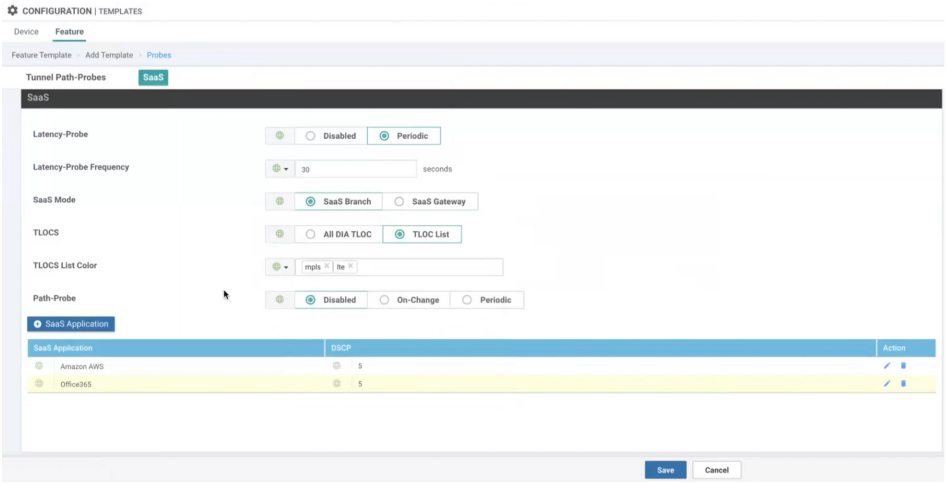
7. Click **SaaS Application** to display the following fields. Use these fields to specify a SaaS application. Repeat the process to add more applications.

   After you specify applications, they appear in a SaaS application table on this window. The table includes an Action column with options to edit or delete applications in the list.

Field	Description
SaaS App	Use the drop-down menu to select an application.
DSCP	**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco SD-WAN Manager CoR SaaS workflow will NOT push this option. The DSCP value provided is not used even when you enable this configuration option. Enter an integer value for the Differentiated Services Code Point (DSCP). A value must be entered, but it is not used by the system. You can assign the same DSCP value to different applications. Range: 0 to 63

8. Click **Save** to save the template.

Example: The example below shows a Probes feature template configured for a branch site, including mpls and lte interfaces; it determines the best path for the Amazon AWS and for Office365 SaaS applications.



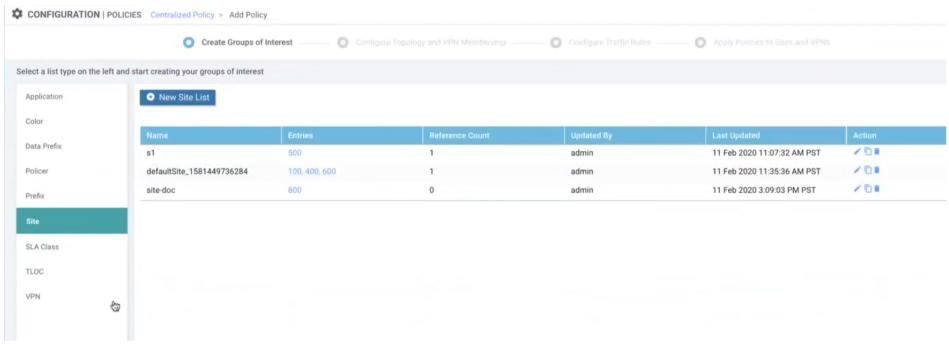
9. To use the feature template in a device template:

   In **Additional Templates** of the device template, in the **Probes** field, choose the feature template created in the mentioned steps.

Create a Policy for Cloud onRamp for SaaS

1. Select **Configuration** > **Policy**.
2. Click the **Centralized Policy** tab.
3. Click **Add Policy**.
4. In the left pane, click **Site**.
5. Create a list of sites to which to apply the policy. The list will be used in a later step.
   a. Click **New Site List**.
   b. In the **Site List Name** field, enter a site list name.
   c. In the **Add Site** field, enter one or more site numbers.
   d. Click **Add**.

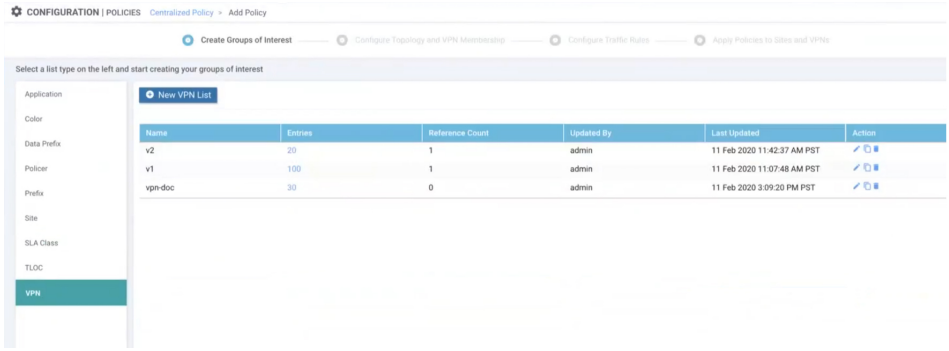
      The site is added to the table of sites.



520449

6. In the left pane, select **VPN**.
7. Create a list of VPNs to which to apply the policy. The list will be used in a later step.
   a. Click **New VPN List**.
   b. In the **VPN List Name** field, enter a VPN list name.
   c. In the **Add VPN** field, enter one or more numbers.
   d. Click **Add**.

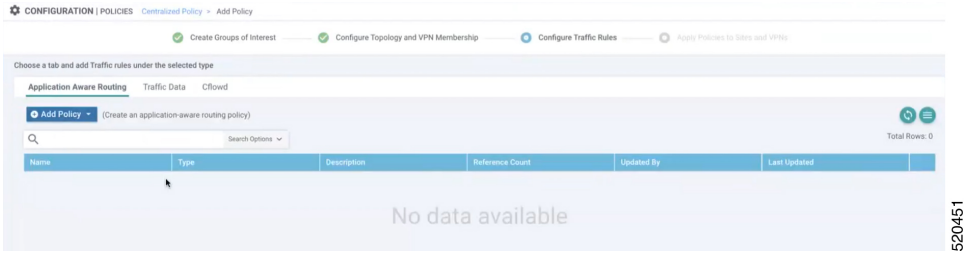
      The VPN is added to the table of VPNs.



520450

8. Click **Next** twice to display the Configure Traffic Rules step.

   The **Application Aware Routing** tab is selected by default.

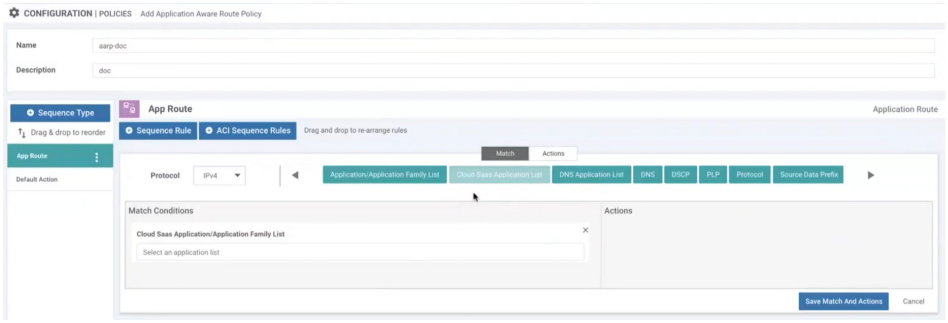


520451

9. Click **Add Policy** and select **Create New**.
10. Create a policy.
    a. Enter a name and description for the policy.
    b. Click **Sequence Type**.

c. Click **Sequence Rule**.

d. With **Match** selected by default, click **Cloud SaaS Application List**.

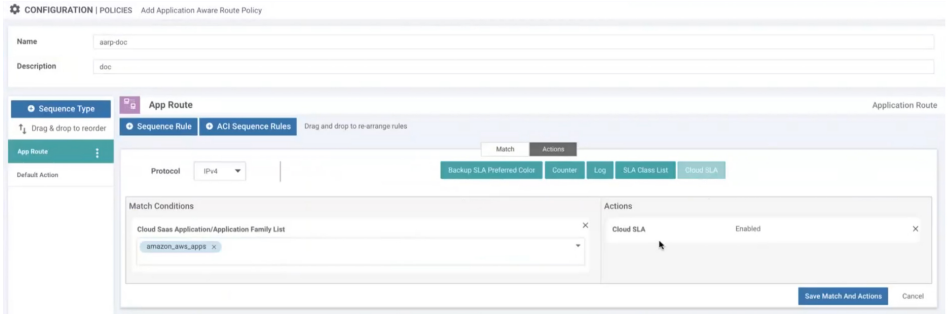


e. In the **Match Conditions** section, specify a SaaS application. Cloud onRamp for SaaS is enabled for this SaaS application.

f. Click **Actions**.

g. Click **Cloud SLA**.

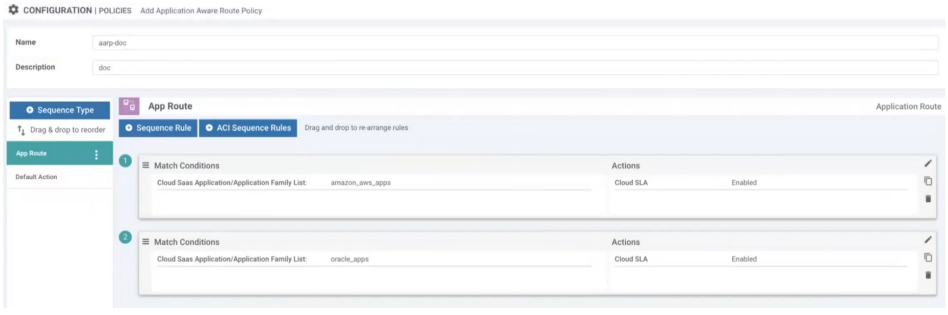
The **Actions** section shows Cloud SLA Enabled.



h. Click **Save Match And Actions**.

i. To add another SaaS application to this policy, click **Sequence Rule** again and follow the steps from 10c.

The following example shows two sequence rules, with Match Condition and Action, each rule specifying a single SaaS application.



j. Click **Save Application Aware Routing Policy**.

k. Click **Next** to display the Apply Policies to Sites and VPNs step.

l. Click the **Application-Aware Routing** tab.

m. Select a policy.

n. Click **New Site List and VPN List**. Select the site list and VPN list created earlier in this procedure.

o. Click **Add**.

p. Click **Save Policy**.

11. Activate the policy.

a. Select **Configuration** > **Policies**.

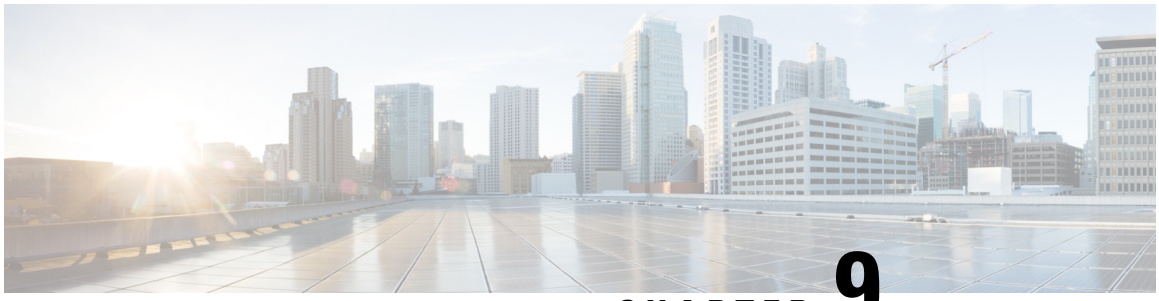
b. In the list of policies, locate the policy to activate. Click the "more actions" (...) button and select **Activate** to push the policy to the devices specified in the policy by site ID.



PART II

Cloud OnRamp for Multicloud (Cisco IOS XE Catalyst SD-WAN Release 17.16.x and Later)

• Cloud OnRamp for Multicloud - Cloud and Interconnect, on page 223



CHAPTER 9

Cloud OnRamp for Multicloud - Cloud and Interconnect

Table 58: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature provides a single common dashboard in Cisco SD-WAN Manager that displays unified information of accounts, gateways, and connections for both cloud and interconnect providers. This feature enhances the experience by helping you identify resources and monitor each provider's utilization.
Enhancements to Enable Connectivity to an Existing AWS Transit Gateway	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature enables you to discover and connect a cloud gateway to an existing AWS Transit Gateway created in the AWS portal.

- Cloud OnRamp for Multicloud, on page 223
- Prerequisites for existing Transit Gateway connectivity, on page 224
- Workflow to Configure Cloud OnRamp for Multicloud, on page 225

Cloud OnRamp for Multicloud

Cloud OnRamp for Multicloud functionalities on Cisco Catalyst SD-WAN Manager Release 20.16.1

The **Cloud OnRamp for Multicloud** page on Cisco SD-WAN Manager:

- Simplifies the experience for multicloud configurations.
- Provides step-by-step, intent-based connectivity deployments that helps you set up the connectivity.

- Provides an onboarding experience for Day 0 configurations and a dashboard experience for Day N configurations.

For a Cisco SD-WAN Manager instance on Cisco Catalyst SD-WAN Manager Release 20.16.1, from the onboarding page you can initially associate a provider account. Once you add an account, you can configure global settings and tags for an associated cloud account. Once you create a connection from the onboarding page, you are automatically switched to the dashboard view. From the dashboard page, click **Go to Onboarding** to go back to the onboarding page.

The **Cloud OnRamp for Multicloud** dashboard shows key utilization metrics for each configured provider:

- Number of accounts
- Number of gateways
- Number of cloud or interconnect connections
- Number of connected tags, applicable only to cloud providers
- If audit is enabled, last status of audit, applicable only to cloud providers

Cloud OnRamp for Multicloud functionalities from Cisco Catalyst SD-WAN Manager Release 20.18.1 and later release

Enhancements to enable connectivity to an existing AWS Transit Gateway

With this feature, you can discover and connect to an existing Transit Gateway that you are maintaining in the AWS portal for your cloud operations. This is done using cloud gateways deployed through Cloud OnRamp for Multicloud in Cisco SD-WAN Manager.

This feature is applicable only to the following solutions:

- Transit Gateway - VPN based
- Transit Gateway - Connect based

If the AWS cloud gateways are created with existing Transit Gateways, the connectivity from the Transit Gateway to the workload VPCs are managed on the AWS portal. For more information, see Configure Transit Gateway connections through AWS portal, on page 263.

You can connect the cloud gateways, comprising of the Cisco Catalyst 8000V, to the Transit Gateways from the Cloud router connectivity tab in the Cloud Connections page.

Prerequisites for existing Transit Gateway connectivity

Transit Gateway in AWS portal

- In the AWS portal, create the Transit Gateway in the AWS region.
- Specify the desired value for AWS **Autonomous System Number** (ASN). Ensure that this value is not the same as Cisco Catalyst 8000V ASN, which is equal to the ASN value in global settings for AWS, plus an offset of 30
- Ensure that the **Default route table association** and the **Default route table propagation** options are not selected.

- Ensure that you select **Auto Accept of Shared Attachments**.

Global network in AWS portal

- In the AWS portal, choose **VPC**> **Network Manager** > **Global Networks** > **Create Global Network** to create a global network.

Register Transit Gateway in AWS portal

- In the AWS portal, register the Transit Gateway with global network.
- In the AWS portal, choose **VPC** > **Network Manager** > **Global Networks** > **Id** which you have created. Click the **Transit Gateway**. Click **Register Transit Gateway** and select the Transit Gateway created by you.

Route table in AWS portal

In the AWS portal, click **VPC** > **Transit Gateway Route Table** in the region where you created the Transit Gateway. Create the route table using this Transit Gateway. Adding tags is optional.

MTU update requirement for Cloud Gateway (CGW) post upgrade

If you upgraded Cisco SD-WAN Manager from an earlier version to Cisco IOS XE Catalyst SD-WAN Release 17.18.1a or later with pre-existing cloud gateways, the existing WAN, S2C, S2S, and IC VPCs might have an MTU of 1460 bytes. Because an N4 CGW requires an Maximum Transmission Unit (MTU) of 1500 bytes, the cloud gateways rejects the bootstrap file and fails to come up. You must update the MTU of all applicable VPCs to 1500 bytes using the GCP CLI before creating an N4 CGW.

When you create a new cloud gateway on Cisco IOS XE Catalyst SD-WAN Release 17.18.1a or later, the workflow automatically provisions VPCs with an MTU of 1500 bytes by default.

Workflow to Configure Cloud OnRamp for Multicloud

1. **Add Accounts**: Associate and manage provider accounts.
2. **Add Global Settings**: Configure and save default settings for provider services.
3. **Add VPCs/VNets Tags**: Discover and tag cloud workloads (VPCs and VNets).
4. **Add Gateway**: Create and manage cloud and interconnect gateways.
5. **Cloud Connections** and Interconnect Connections, on page 264: You can establish site-to-site, site-to-cloud, and cloud-to-cloud connectivity through the dashboard after bringing up the first gateway.

   Once you create a connection from the onboarding page, you are automatically switched to the dashboard view.

Manage Accounts

Add an AWS Cloud Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

     From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose provider as **AWS** or **AWS Gov Cloud** based on your requirement.
3. Enter the following parameters:

Field	Description
Account name	Enter the account name.
Description (Optional)	Enter the description.
Use for cloud gateway	Choose **Yes** if you want to create cloud gateway in your account, or choose **No**.
Login in to AWS with	Choose the authentication model you want to use: • **Key** • **IAM Role**

4. If you choose the **Key** model, then provide **API Key** and **Secret Key** in the respective fileds.

   Or

   If you choose the **IAM Role** model, then create an IAM role with Cisco SD-WAN Manager provided **External ID**. Note the displayed **External ID** from the window and provide the **Role Amazon Resource Name (ARN)** value that is available when creating an IAM role.

   Choose **IAM Role** only if the controllers are deployed in AWS. If the controllers are managed by Cisco but deployed in AWS, use the **External ID**.

   To create an IAM role, you must enter the External ID provided by Cisco SD-WAN Manager into a policy by using the AWS Management Console. Do the following:

   a. Attach an IAM Role to an existing Cisco SD-WAN Manager EC2 instance.

      1. See the Creating an IAM role (console) topic of AWS documentation to create a policy. In the AWS **Create policy** wizard, click **JSON** and enter the following JSON policy document.

```
{

"Version": "2012-10-17",

  "Statement": [{
```

```
        "Sid": "VisualEditor0",
    "Effect": "Allow",
        "Action": "sts:AssumeRole",
    "Resource": "*"
        }
    ]
    }
```

2. See the Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console blog of AWS Security Blog for information about creating an IAM role and attaching it to the Cisco SD-WAN Manager EC2 instance based on the policy created in Step 1.

Note On the **Attach permissions policy** window, choose the AWS managed policy that you created in Step 1.

Note The following set of permissions are allowed:

- AmazonEC2FullAccess
- IAMReadOnlyAccess
- AWSNetworkManagerFullAccess
- AWSResourceAccessManagerFullAccess

For more information on creating an AWS IAM Role, refer Creating an AWS IAM Role.

b. Create an IAM role on an AWS account that you want to use for the multicloud environment.

1. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require External ID** and pasting the external ID.
2. See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

   In the **IAM Roles** window, scroll down and click the role you created in the previous step.

   In the **Summary** window, note the **Role Amazon Resource Name (ARN)** that is displayed at the top.

Note You can enter this role ARN value when you choose the authentication model as IAM role in Step 7.

3. After modifying the trust relationship, click **JSON** and enter the following JSON document. Save the changes.

Note The account Id in the following JSON document belongs to the Cisco SD-WAN Manager EC2 instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
       }
      }
    }
  ]
}
```

5. Click **Submit**.

To view or update the account details, click **...** on the **Manage Accounts** page.

You can also remove the account if there are no associated host VPC tags or cloud gateways.

Note During the Multicloud resource cleanup process, Cisco SD-WAN Manager compares the current database to the running resources in the account using the organisation name and account detail tags. Any resources that match the tags but are not in the current database are deleted. Therefore, the AWS Multicloud resources of Cisco SD-WAN Manager can be deleted by another Cisco SD-WAN Manager if the organization name and the associated AWS account details are the same. We recommend that if you are using the same AWS account across different Cisco SD-WAN Manager overlays, ensure that you use different organization and overlay name for each Cisco SD-WAN Manager.

Add an Azure Cloud Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

     From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Azure** or **Azure Gov Cloud** based on your requirement.
3. Enter the following information:

Field	Description
Account name	Enter a name for your Azure subscription.
Description (optional)	Enter a description for the account. This field is optional.
Use for cloud gateway	Choose **Yes** to designate the account to be used for cloud gateway creation. The option **Yes** is chosen by default.
Tenant ID	Enter the ID of your Azure Active Directory (AD). To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use as part of this workflow.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret key	Enter the password associated with the client ID.

4. Click **Submit**.

Add a Google Cloud Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

     From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Google Cloud**.
3. Enter the following information:

Field	Description
Account name	Enter a name for your Google Cloud account.
Description (optional)	Enter a description for the account.
Use for cloud gateway	Choose **Yes** to create a cloud gateway in your account. The option **Yes** is chosen by default.

Field	Description
Billing ID (Optional)	Enter the billing ID associated with your Google Cloud service account. If you provide a billing ID, it goes through an automatic validation process. **Note** This field is visible only if you choose the **Yes** option for the **Use for Cloud Gateway** field.
Service directory lookup	Choose **Yes** to allow Cisco SD-WAN Manager to discover services or applications in the Google Service Directory associated with the Cloud Account. The option **No** is chosen by default.
Private key ID	Click **Upload Credential File**. You must generate this file by logging in to Google Cloud console. The private key ID may be in JSON or REST API formats. The format depends on the method of key generation. For more details, see Google Cloud documentation. For more information, see Cisco SD-WAN Cloud onRamp for Multicloud using Google Cloud Platform.

4. Click **Submit**.

Associate a Megaport Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

     From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Megaport**.
3. Configure the following:

Field	Description
Account name	Enter a name of your choice. This name is used to identify the Megaport account in workflows that define the cloud or site-to-site interconnects.
Description (Optional)	Enter a description.
User name	Enter the username of your Megaport account.

Field	Description
Password	Enter the password of your Megaport account.
Customer key	(Supported releases: Cisco Catalyst SD-WAN Manager Release 20.18.1 and later) Enter the API key of your Megaport account.
Customer secret	(Supported releases: Cisco Catalyst SD-WAN Manager Release 20.18.1 and later) Enter the API secret of your Megaport account.

Note

- Use of **User name** and **Password** is deprecated from Cisco Catalyst SD-WAN Manager Release 20.18.1.
- New Megaport account association authentication is via **Customer key** and **Customer secret**.
- If you upgrade Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.18.1 and you already have associated Megaport accounts via **User name** and **Password**, the associations continue to work. To reauthenticate, you must use an API key and secret generated for the same account, as username and password authentication is not supported.

4. Click **Submit**.

Cisco SD-WAN Manager authenticates the account and saves the account details in a database.

Associate an Equinix Account

1. You can associate provider accounts in two ways:
   - If you are a first-time user:

     From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

     From the onboarding page, click **Add accounts**.
   - Alternatively, from the dashboard page click **Manage Accounts**.

     Click **Add accounts**.
2. Choose **Equinix**.
3. Configure the following:

Account name	Enter a name of your choice. This name is used to identify the Equinix account in workflows that define the cloud or site-to-site interconnects.
Description (Optional)	Enter a description.
Customer key	Enter the client ID (consumer key).
Customer secret	Enter the client secret key (consumer secret).

4. Click **Submit**.

Cisco SD-WAN Manager authenticates the account and saves the account details in a database.

Global Settings

The global settings for each provider includes mandatory fields. The **Advanced layout** option provides all the advanced settings with preconfigured values. If you do not explicitly select a value in the fields that appear when you enable **Advanced layout**, preconfigured values are chosen. The **Advanced layout** option is disabled by default.

Configure Global Settings for AWS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   On the onboarding page, click **Add global settings**.

2. Configure the settings based on your requirements:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices. **Note** Configuration groups is not supported on AWS Branch Connect solution.

Field	Description
Cloud gateway solution	From the drop-down list choose one of the following options: • **Transit Gateway–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach. • **Transit Gateway–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS TGW Connect (GRE tunnels) approach. • **Transit Gateway–Branch-connect**—Allows connectivity of different Cisco Catalyst SD-WAN edge devices to VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. This option uses the AWS VPN connection (IPSec) approach. • **Cloud WAN–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach. • **Cloud WAN–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS Connect attachments (supporting GRE tunnels) approach.

Field	Description
Reference account name	From the drop-down list choose the reference account name. Cisco SD-WAN Manager discovers the software images and instance sizes using this reference account name. **Note** You can still choose a different account, if required, at the time of a cloud gateway creation.
Reference region	From the drop-down list choose the reference region. Cisco SD-WAN Manager discovers the software images and instance sizes in this reference region under the referenced account name.
License type	Choose **BYOL** to use a bring your own license software image
	Choose **PAYG** to use a pay as you go software image. **Note** **PAYG** is supported only on Transit Gateway - VPN based and Connect based solutions.
Software image	From the drop-down list, select a software image.
Instance size	From the drop-down list choose the required size.
IP subnet pool	Enter the subnet pool address. You cannot modify the pool when a few cloud gateways are already making use of pool.
Full mesh of transit VPCs	Specifies the full mesh connectivity between TVPCs of cloud gateways in different regions to carry site to site traffic (through Cisco Catalyst 8000V).

Field	Description
Tunnel count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list. Enter the number of tunnels for a GRE/peer connection. You can configure up to 4 tunnels for each GRE/peer connection. Each tunnel supports up to 5 Gbps of traffic. **Note** Changing the value of this parameter does not affect existing cloud gateways. To update the tunnel count for an existing cloud gateway, edit the cloud gateway from the **Configuration** > **Cloud OnRamp For Multicloud** > **Cloud Gateway** page.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
BGP ASN	Specifies the offset for allocation of transit gateway BGP ASNs. It is used to block routes learnt from one transit gateway (eBGP) to another. A band of 30 ASNs are reserved for transit gateway ASNs. Starting offset plus 30 will be the organization side BGP ASN. For example, if the offset is 64830, Org BGP ASN will be 64860. Acceptable start offset range is 64520 to 65500. It must be a multiple of 10.
Intra tag communication	Specifies if the communication between host VPCs under the same tag is enabled or disabled. If any tagged VPCs are already present and cloud gateways exist in those regions, then this flag cannot be changed.
Program default route in VPCs towards TGW/Core network	Specifies if the main route table of the host VPCs is programmed with default route is enabled or disabled.
Enable periodic audit	If you enable the periodic audit, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.

Field	Description
Enable auto correct	If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.

Click **Save**.

Configure Global Settings for Azure and Azure Gov Cloud

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   On the onboarding page, click **Add global settings**.

2. Configure the global settings:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices in the multicloud workflow. **Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers.
Software image	Choose the software image of the WAN edge device to be used in the Azure Virtual Hub. **Note** Choose the Cisco Catalyst 8000V image based on your Cisco SD-WAN Manager release.
SKU scale	From the drop-down list, choose a scale based on your capacity requirements.

Field	Description
IP subnet pool	Specify the IP subnet pool to be used for the Azure virtual WAN hub. A subnet pool needs prefixes between /16 and /24. A single /24 subnet pool is able to support one cloud gateway only. You cannot modify the pool if other cloud gateways are already using the pool. Overlapping subnets are not allowed. The IP subnet pool is meant for all Azure Virtual WAN Hubs inside an Azure Virtual WAN, one /24 prefix per Virtual WAN Hub. Ensure that you allocate enough /24 subnets for all the Virtual WAN Hubs you plan to create within the Virtual WAN. If a Virtual WAN Hub is already created in Microsoft Azure, you can discover it through Cisco SD-WAN Manager and use the existing subnet pool for the discovered hub.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
BGP ASN	Specify the ASN to be used by the cloud gateway for eBGP peering with the virtual hub.
Advertise default route to Azure Virtual Hub	By default, this field is **Disabled**. If you click **Enabled**, the internet traffic from the virtual network is redirected through Cisco Catalyst SD-WAN branches
Enable periodic audit	If you enable the periodic audit, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.
Enable auto correct	If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.
Push monitoring metrics to Azure	For the field, choose **Enabled** or **Disabled**. If you choose **Enabled**, the cloud gateway metrics associated with your Azure subscription are sent to the Microsoft Azure Monitoring Service portal periodically. These metrics are sent in a format prescribed by Microsoft Azure for all NVA vendors. This option is not available for Azure Gov Cloud.

Click **Save**.

Configure Global Settings for Google Cloud

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   On the onboarding page, click **Add global settings**.

2. Configure the global settings:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices.
Software image	Choose the software image of the WAN edge device for the WAN VPC. This should be a preinstalled Cisco Catalyst 8000V instance.
Instance size	Choose an instance based on your requirements.
IP subnet pool	Specify the IP subnet pool for the SD-WAN cloud gateway in Google Cloud. This subnet pool needs prefixes between /16 and /21. **Note** The IP subnet pool cannot be modified after a cloud gateway is created.
BGP ASN	Specify the autonomous system number (ASN) for the cloud gateway for BGP peering. This is the starting offset for the allocation of ASNs for the cloud gateways and Google Cloud routers. Starting from the offset, 10 ASN values are reserved for allocating to the cloud gateways. **Note** This offset value cannot be modified after a cloud gateway is created.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Intra tag communication	If enabled, the VPCs with the same tag can communicate with each other.
Site-to-site communication	Enable for site-to-site transit connectivity using the Google global network.
Site-to-site tunnel encapsulation type	Choose the encapsulation from the drop-down list.

Service directory lookup capable	Enable to allow Cisco SD-WAN Manager to discover Google Service Directory applications associated with this Google account.
Network service tier	Choose one of the Google Cloud service tiers. • PREMIUM: Provides high-performing network experience using Google global network. • STANDARD: Allows control over network costs.
Enable periodic audit	If you enable the periodic audit, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.
Enable auto correct	If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.

Click **Save**.

Configure Global Settings for Megaport

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   On the onboarding page, click **Add global settings**.

2. Configure the following:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default.
Software image	Choose a Cisco Catalyst 8000V image.
Instance size	Instance Size determines the compute footprint and throughput of each Cisco Catalyst 8000V instance. Choose one of the following: • **Small** • **Medium** • **Large**
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
Interconnect transit color	Select the color to assign for the connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
Interconnect CGW SDWAN color	Choose the color to be used for the interface through which the Interconnect Gateway connects to the Cloud Gateway. **Note** Color assigned to an interface must be unique for the Interconnect Gateway devices and common across Cloud Interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway, and Cloud Gateway.

Click **Save**.

Configure Global Settings for Equinix

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   On the onboarding page, click **Add global settings**.

2. Configure the following:

Field	Description
Enable configuration group	Enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default.
Software image	Choose a Cisco Catalyst 8000V image.
Instance size	Instance Size determines the compute footprint and throughput of each Cisco Catalyst 8000V instance. Choose one of the following: • **Small** • **Medium** • **Large** • **xLarge**

Field	Description
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

Advanced Layout

If you enable the **Advanced layout** option, configure the following:

Field	Description
Interconnect transit color	Select the color to assign for the connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
Interconnect CGW SDWAN color	Choose the color to be used for the interface through which the Interconnect Gateway connects to the Cloud Gateway. **Note** Color assigned to an interface must be unique for the Interconnect Gateway devices and common across Cloud Interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway, and Cloud Gateway.

Click **Save**.

Add VPCs/VNets Tags

After you associate an account with Cisco SD-WAN Manager, you can discover host VPCs or VNets in the regions associated with the account. You can create new tags for the discovered VPCs or VNets, or modify or delete existing tags. Tags are used to manage connectivity between the VPCs or VNets and Cisco Catalyst SD-WAN branch VPNs.

Create Tags for AWS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   In the onboarding page, click **Add VPC/VNet tags**. Choose the provider and click **Next**.

   Alternatively, you can navigate to the **VPC/VNet tags** page from the Cloud OnRamp for Multicloud dashboard. Click **Add tag**.

2. Enter a **Tag name**.
3. Choose a **Cloud region** from the drop-down list.
4. To use the VPC tag while creating a cloud interconnect connection to a provider, **Enable for Middle-Mile partner Interconnect Connections** . If enabled, the tag can only be used for interconnect connections and is not available for cloud gateway intent mapping.
5. Select the host VPCs from the table and view the **Selected VPCs**.
6. Click **Add**.

In the **VPC/VNet Tags** page, you can toggle between tags and VPCs. A list of discovered host VPCs and tags displays in a table with the following columns: Tag Name, Cloud Region, Account Name, Associated VPCs, and Interconnect Enabled.

For the tags, click **...** under **Action** column to:

- **Edit**: Change the selected VPCs for an existing tag.
- **Delete**: Delete the tag for the selected VPC.

Create Tags for Azure and Azure Gov Cloud

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   In the onboarding page, click **Add VPC/VNet tags**. Choose the provider and click **Next**.

   Alternatively, you can navigate to the **VPC/VNet tags** page from the Cloud OnRamp for Multicloud dashboard. Click **Add tag**.
2. Enter a **Tag name**.
3. Choose a **Cloud region** from the drop-down list.
4. To use the VNet tag while creating a cloud interconnect connection to a provider, **Enable for Middle-Mile partner Interconnect Connections** . If enabled, the tag can only be used for interconnect connections and is not available for cloud gateway intent mapping.
5. Select the VNets from the table and view the **Selected VNets**.
6. You can choose the **Cloud gateway attachment** as **Auto** or map with an existing cloud gateway. The **Auto** option is automatically selected for **Cloud gateway attachment**.
7. Click **Add**.

In the **VPC/VNet Tags** page, you can toggle between tags and VNets. A list of discovered host VNets displays in a table with the following columns: Tag Name, Cloud Gateway Attachment, Account Name, Cloud Region, Interconnect Enabled, and VNet Name.

For the tags, click **...** under **Action** column to:

- **Edit**: Change the selected VNets for an existing tag.
- **Delete**: Delete the tag for the selected VNet.

Create Tags for Google Cloud

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   In the onboarding page, click **Add VPC/VNet tags**. Choose the provider and click **Next**.

   Alternatively, you can navigate to the **VPC/VNet tags** page from the Cloud OnRamp for Multicloud dashboard. Click **Add tag**.
2. Enter a **Tag name**.
3. Choose a **Cloud region** from the drop-down list.
4. Select the host VPCs from the table and view the **Selected VPCs**.
5. Click **Add**.

In the **VPC/VNet Tags** page, you can toggle between tags and VPCs. A list of discovered host VPCs and tags displays in a table with the following columns: Tag Name, Cloud Region, Account Name, Associated VPCs, and Interconnect Enabled.

For the tags, click **...** under **Action** column to:

- **Edit**: Change the selected VPCs for an existing tag.
- **Delete**: Delete the tag for the selected VPC.

Note You cannot create a tag with multiple regions. To add more regions to a tag, you must first create a tag with one region and then edit the tag to add a new region.

Create and Manage Gateways

Create and Manage Cloud Gateways

Create AWS Cloud Gateway

Note You cannot create multiple AWS cloud gateways in a single region.

To create a cloud gateway, perform the following steps.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.
2. Select the provider:

Field	Description
Provider	Choose **AWS** from the drop-down list.
Account name	Choose the account name from the drop-down list.
Cloud gateway name	Enter the cloud gateway name.
Description(Optional)	Enter the description.
Region	Choose the region from the drop-down list.
Transit gateway	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Select one of the options: • **Create new**: Creates a new Transit Gateway and a transit VPC with a pair of virtual routers. • **Connect later/skip connection**: Creates transit VPC with a pair of virtual routers without creating a new Transit Gateway or any attachments to an existing one. You can later attach this cloud gateway to an existing Transit Gateway using SD-WAN Manager, or manually. You can either bring up attachments to the Transit Gateway through the Edit Gateway page, or through the Cloud router connectivity tab on the Cloud Connections page, once the cloud gateway is associated with an existing Transit Gateway from the Edit Gateway page. • **Use existing**: Creates a transit VPC of virtual routers. You can select an existing Transit Gateway which was created in the AWS portal. Click **Add attachments** to connect the virtual routers in the transit VPC to the Transit Gateway and associate the SD-WAN Manager VPN to the Transit Gateway route table that you have created from the AWS portal. If you choose **Connect later/skip connection** or **Use existing**, to connect the Transit Gateway with the workload VPC , see Configure Transit Gateway connections through AWS portal, on page 263.

Note If you are using an existing Transit gateway and want to create a cloud gateway using **Create new**, then perform these steps to avoid creating two separate Global Networks—one for the existing Transit Gateway and one for the new Transit Gateway:

a. Create a new cloud gateway.

b. Deregister Transit Gateway from the AWS Global Network manually created in the AWS portal.

c. Register the Transit Gateway (deregistered in step b) with the Global Network created by Cisco SD-WAN Manager.

It is recommended to disable audit if you are using the existing and new Transit Gateways together. You must also disable auto-correct option.

Click **Next**.

3. Configure the site parameters:

Field	Description
SSH key (Optional)	Choose the SSH Key from the drop-down list.
Site name	Choose a site for which you want to create the cloud gateway.
Configuration group	**Note** When you enable configuration groups, it is enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers. If you have enabled the **Enable Configuration Group** option in the AWS global settings, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow.

Field	Description
Chassis number	Associate a pair of chassis to the configuration group.
Instance settings	
License type	Choose a licensing option: • **BYOL** for bring your own license. • **PAYG** for pay as you go.
Software image	From the drop-down menu, choose a software image. **Note** The software image options are determined by the selection of **BYOL** or **PAYG**.
Instance size	From the drop-down list, choose the required size. Pick the size of the WAN edge based on the capacity needs.
IP subnet pool	Enter the subnet pool address. Subnet pool is used for transit VPC creation, needs between /16 to /24.System allocates /27 per transit VPC 8 subnet(s).
Tunnel count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list in the global settings for AWS. Enter the number of tunnels for a VPN connection.
This option is available only when Multi-Region Fabric is enabled. **Multi-Region Fabric Settings**	
MRF role	Choose **Border** or **Edge**.

Click **Next**.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

   Most of the parameters are auto-populated based on your eariler selections. Click the edit icon for each chassis number to modify the following:

   - **System IP**
   - **Host name**
   - **WAN region**
   - **TLOC color**

- **Username**
- **User password**

Click **Next**.

5. Verify all the configuration parameters and click **Deploy**.

Note Creating cloud gateways for AWS Cloud WAN can take over an hour depending on the resources deployed. The first deployment in a region may fail due to AWS's resource verification and validation processes in that region.

You cannot create cloud gateways in regions that do not support AWS Cloud WAN. For information about currently supported regions, see the AWS documentation.

You cannot edit a configuration group created in a multicloud workflow outside of a multicloud workflow.

Create Cloud Gateway for Azure and Azure Gov Cloud

Creation of cloud gateways involves the instantiation or discovery of Azure Virtual WAN Hub and creation of two or more Cisco Catalyst 8000V instances within the hub.

Note If you have used the Azure portal to provision Cisco Catalyst 8000V instances, and created an Azure Virtual WAN and Azure Virtual WAN Hub using the Azure portal, you can also discover them using the procedure below.

To create a cloud gateway, perform the following steps.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. Select the provider:

Field	Description
Provider	Choose **Azure** from the drop-down list.
Account name	Choose your Azure account name from the drop-down list.

Field	Description
Cloud gateway name	Enter the name of your cloud gateway. **Note** If you have created an Azure Virtual WAN Hub using the Azure portal, ensure that you enter the exact virtual hub name in this field. This ensures that the resources associated with the hub are discovered. The associated Azure Virtual WAN and Azure Virtual WAN Hub then become available for you to choose from in the **Azure Virtual WAN** and **Azure Virtual WAN Hub** fields.
Description (Optional)	Enter a description for the cloud gateway.
Region	Choose an Azure region from the drop-down list.

Field	Description
Resource group	Perform one of these actions: • Choose a resource group from the drop-down list • Choose **Create New**. For more information, see Create resource groups. **Note** If you choose to create a new resource group, you also need to create a new Azure virtual WAN and an Azure virtual WAN hub.
Azure Virtual WAN	Perform one of these actions: • Choose an Azure Virtual WAN from the drop-down list. • Click **Create New** to create a new Azure Virtual WAN.
Azure Virtual WAN Hub	Perform one of these actions: • Choose an Azure Virtual WAN Hub from the drop-down list. • Click **Create New** to create a new Azure virtual WAN hub.

Click **Next**.

3. Configure the site parameters:

Field	Description
Solution type	Choose one of the solution type from the drop-down list: • **vHub with NVA** • **vHub with VPN** **Note** You cannot configure both the VPN and NVA solutions in the same region. Also, you cannot configure more than one VPN Gateway in the same region.

If you choose **vHub with NVA** configure the following parameters:

Field	Description
Site name	From the drop-down list, choose a site for which you want to create the interconnect gateway or click **Create New**. If you click **Create New**, configure the site settings in the slide-in pane. You can create a new site only if you have enabled configuration groups in the global settings. Configure the following and click **Save**: • **Name** • **Description** (optional) • **Site ID** (optional) • **Country** (optional) • **Address** (optional) • **City** (optional) • **State** (optional) • **Zip code** (optional)

Field	Description
Configuration group	If you have enabled the **Enable Configuration Group** option in the Azure global settings, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow.
Chassis number	Associate the number of chassis based on your requirement to the configuration group.
Instance settings	
Software image	This field is auto-populated with the configurations from the global settings. You can modify this field based on your requirements.
IP subnet pool	This field is auto-populated with the configurations from the global settings. You can modify this field based on your requirements.
SKU scale	This field is auto-populated with the configurations from the global settings. You can modify this field based on your requirements.
This option is available only when Multi-Region Fabric is enabled. **Multi-Region Fabric Settings**	
MRF role	Choose **Border** or **Edge**.

Click **Next** to proceed to step 3.

If you choose **vHub with VPN** configure the following parameters:

Note You can create only one gateway for VPN solution in one region.

Field	Description
SKU scale	This field is auto-populated with the configurations from the global settings when you onboard the virtual hubs with Cisco Catalyst 8000V created on Cisco SD-WAN Manager. You can modify this field based on your requirements.
IP subnet pool	This field is auto-populated with the configurations from the global settings when you onboard the virtual hubs with Cisco Catalyst 8000V created on Cisco SD-WAN Manager. You can modify this field based on your requirements.

Click **Next** to proceed to step 4.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

   Most of the parameters are auto-populated based on your eariler selections. Click the edit icon for each chassis number to modify the following:

   - **System IP**
   - **Host name**
   - **WAN region** (This option is available only when Multi-Region Fabric is enabled.)
   - **TLOC color**
   - **Username**
   - **User password**

   Click **Next**.

5. Review the connection summary. Click **Deploy**.

Note It can take up to 40 minutes for your Azure Virtual WAN hub to be created and for the Cisco SD-WAN Manager instances to be provisioned inside the virtual hub.

Note Once the creation of the Azure Virtual WAN Hub is complete, you have the option to convert it into a secured Azure Virtual WAN Hub. However, this configuration can only be completed through the Microsoft Azure portal. See Microsoft Azure documentation for more information.

Note You can simultaneously create Azure cloud gateways in different regions.

- Before creating multiple cloud gateways in different regions, create the resource group, virtual WAN, and storage account for the first cloud gateway.
- Before creating multiple cloud gateways in the same region, create the virtual hub for the first cloud gateway in the region.
- You need to have blob access to create a storage account in Azure for the Cloud OnRamp for Multicloud. Blob access is required while creating cloud gateways and modifying scale operations on the Cisco Catalyst SD-WAN devices.

Note The Cloud OnRamp for Multicloud workflow supports up to eight virtual hubs in each Azure region. You can deploy only one cloud gateway Network Virtual Appliances (NVAs) in each virtual hub which supports upto five devices.

Note You cannot edit configuration groups created by multicloud workflows outside of multicloud workflows.

Create Google Cloud Gateways

When the first cloud gateway is created, three reserved VPCs are instantiated—WAN transit VPC, site-to-site transit VPC, and site-to-cloud transit VPC. Cisco Catalyst 8000V instances that are instantiated as part of the cloud gateway are anchored to the VPCs.

Note You cannot use the same configuration group for more than one cloud gateway in Google Cloud and AWS. Use different configuration groups for each cloud gateway in Google Cloud and AWS.

To create a cloud gateway, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. Enter the provider details:

Field	Description
Provider	Choose **Google Cloud** from the drop-down list.
Account name	Chose your Google Cloud account name from the drop-down list.

Field	Description
Cloud gateway name	Enter a name for your cloud gateway. **Note** Ensure that the name is in lower case letters. See the Google Cloud documentation for information about Naming resources and Naming convention.
Region	Choose a Google region from the drop-down list.
Description (Optional)	Enter a description.
Involved in site-to-site communication	If the cloud gateway will participate in site-to-site communication, click **Yes**. If the cloud gateway will not participate in site-to-site communication, click **No**. **Note** This field is enabled for configuration only when **Site-to-site Communication** is enabled in the global settings. When **Site-to-site Communication** is disabled in the global settings, this field is dimmed.

Click **Next**.

3. Configure the site parameters:

Field	Description
NHM region (This option is available only when Multi-Region Fabric is enabled.)	From the drop-down list, choose a network health monitoring (NHM) region for which you want to create the gateway.
Site name	From the drop-down list, choose a site for which you want to create the cloud gateway.

Field	Description
Configuration group	**Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers. If you have enabled the **Enable Configuration Group** option in the Google Cloud global settings, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow.
Chassis number	You can associate between 2 and 8 chassis to the configuration group
Instance settings	
Software image	From the drop-down menu, choose a software image.
Instance size	From the drop-down list, choose the required size. Pick the size of the WAN edge based on the capacity needs.
IP subnet pool	Enter the subnet pool address. Subnet pool is used for transit VPC creation, needs between /16 to /24.System allocates /27 per transit VPC 8 subnet(s).
Network service tier	Choose one of the Google Cloud network service tiers from the drop-down list. • **PREMIUM**: Provides high-performing network experience using Google Cloud global network. • **STANDARD**: Allows control over network costs.

Field	Description
This option is available only when Multi-Region Fabric is enabled. **Multi-Region Fabric Settings**	
MRF role	Choose **Border** or **Edge**.

Click **Next**.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

   Most of the parameters are auto-populated based on your eariler selections. Click the edit icon for each chassis number to modify the following:

   - **System IP**
   - **Host name**
   - **WAN region** (This option is available only when Multi-Region Fabric is enabled.)
   - **TLOC color**
   - **Username**
   - **User password**

   Click **Next**.

5. Click **Deploy**.

View, edit, or delete a cloud gateway

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud.**

Step 2 Click **Gateway Management** on the Cloud OnRamp for Multicloud dashboard.

Existing cloud gateway details are summarized in a table.

Step 3 In the table, click **…** for the desired cloud gateway.

- To view more information about the cloud gateway, click **View**.
- To delete the cloud gateway, click **Delete** and confirm that you wish to delete the gateway.
- To edit the cloud gateway, click **Edit**. You can edit the tunnel count of the cloud gateway

  From Cisco Catalyst SD-WAN Manager Release 20.18.1, when you connect to an existing Transit Gateway, you can create VPN attachments and update the tunnel count when you edit an AWS cloud gateway.

  To disconnect the Transit Gateway connections and to connect later click **Disconnect**.

  To connect a transit VPC including a pair of virtual routers with an existing Transit Gateway, click **Use existing**. You can discover a Transit Gateway from the cloud gateway's region and attach chosen VPN(s) with Transit Gateways

routing tables. You can also add attachments in Cloud Connections page. For more information, see Cloud router connectivity.

Create and Manage Interconnect Gateways

Create a Gateway at a Megaport Location

Deploy a Cisco Catalyst 8000V instance as the interconnect gateway at the desired Megaport location. We recommend that you deploy the Cisco Catalyst 8000V instance at the Megaport location closest to your branch location.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. To view the Interconnect Gateway licenses purchased through Cisco, that are associated with the account, click **Check available licenses**.

   Configure the following provider parameters:

Field	Description
Provider	Choose **Megaport**.
Account name	Choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Interconnect gateway name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.

3. Configure the site parameters:

Field	Description
Location	Choose the Megaport PoP location where the Cisco 8000v instance must be deployed.

Field	Description
Provider license type	• **Prepaid**: Choose a prepaid license type to create the interconnect gateway. • **PayG**: Choose a pay-as-you-go (PAYG) license type to create the interconnect gateway. **Note** When using a Megaport account with Cisco billing, specify if you want to use a prepaid MVE license, or PAYG license where you are billed for each month. The selection must be done at the time of gateway creation and cannot be changed later. Appropriate prepaid or PAYG license should be purchased beforehand.
Internet bandwidth (IP transit) in Mbps	Choose the IP transit bandwidth value.
WAN region	This option is available only when Multi-Region Fabric is enabled. From the drop-down list, choose a WAN region for which you want to create the interconnect gateway.
Site name	From the drop-down list, choose a site for which you want to create the interconnect gateway or click **Create New**. If you click **Create New**, configure the site settings in the slide-in pane. You can create a new site only if you have enabled configuration groups in the global settings. Configure the following and click **Save**: • **Name** • **Description** (optional) • **Site ID** (optional) • **Country** (optional) • **Address** (optional) • **City** (optional) • **State** (optional) • **Zip code** (optional)

Field	Description
Configuration group	If you enabled the **Enable Configuration Group** in global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups. **Note** It does not include other configuration groups that are created in Cisco SD-WAN Manager. The configuration groups in this drop-down list include the options that are needed for this provider.
Chassis number	Choose the chassis number of a Cisco Catalyst 8000v instance that has the Megaport default template attached. If the configuration group is enabled, Cisco Catalyst 8000v chassis numbers do not require the Megaport template to be attached. **Note** The chassis numbers are auto-populated when you choose a site from the **Site Name** drop-down list.
Instance settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect global settings. • **Custom**: Choose a specific instance size and software image for this gateway.
MRF role	This option is available only when Multi-Region Fabric is enabled. Choose a router role: **Border** or **Edge**.
Transport gateway	This option is available only when Multi-Region Fabric is enabled. Choose **Enabled** or **Disabled**.

4. This step is applicable only when you enable configuration groups.

   Configure the device parameters:

The system IP address is not auto-populated for the interconnect connections. Click the edit icon for the chassis number to modify the following:

- **System IP**
- **Host name**
- **Color**
- **Username**
- **User password**

Click **Next**.

5. Click **Deploy**.

When the configuration task is successful, the interconnect gateway is listed in the **Gateway Management** page.

Create a Gateway at a Equinix Location

Deploy a Cisco Catalyst 8000V instance as the interconnect gateway at the desired Equinix location. We recommend that you deploy the Cisco Catalyst 8000V instance at the Equinix location closest to your branch location.

If a subscription for Equinix SKUs is purchased through Cisco and the account is associated to the subscription via the Equinix portal, then all network edges brought up by the Cisco SD-WAN Controller, along with the IP transit associated with those network edges, device link groups, and all virtual connections originating from those network edges, is billed by Cisco. Otherwise, these component SKUs are billed directly by Equinix.

To create an interconnect gateway, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   Click **Onboarding** and then click **Add gateway**.

   Alternatively, you can also create gateways from the **Gateway Management** tab on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.

2. Configure the following provider parameters:

Field	Description
Provider	Choose **Equinix**.
Account name	Choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Gateway name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.

3. Configure the site parameters.

Field	Description
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Equinix metro location where the Cisco 8000v instance must be deployed.
Billing Account ID	Choose the appropriate billing account for the location.
WAN region	This option is available only when Multi-Region Fabric is enabled. From the drop-down list, choose a WAN region for which you want to create the interconnect gateway.
Site name	From the drop-down list, choose a site for which you want to create the interconnect gateway or click **Create New**. If you click **Create New**, configure the site settings in the slide-in pane. You can create a new site only if you have enabled configuration groups in the global settings. Configure the following and click **Save**: • **Name** • **Description** (optional) • **Site ID** (optional) • **Country** (optional) • **Address** (optional) • **City** (optional) • **State** (optional) • **Zip code** (optional)

Field	Description
Configuration group	If you enabled the **Enable Configuration Group** in global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. **Note** You can only choose configuration groups created from the create new workflow. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups. **Note** The **Configuration Group** drop-down list includes only configuration groups that you create from this drop-down list. It does not include other configuration groups that are created in Cisco SD-WAN Manager. The configuration groups in this drop-down list include the options that are needed for this provider.
Chassis number	Choose the chassis number of a Cisco Catalyst 8000v instance that has the Equinix default template attached. If the configuration group is enabled, Cisco Catalyst 8000v chassis numbers do not require the Equinix template to be attached. **Note** The chassis numbers are auto-populated when you choose a site from the **Site Name** drop-down list.
Instance settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect global settings. • **Custom**: Choose a specific instance size and software image for this gateway.
MRF role	This option is available only when Multi-Region Fabric is enabled. Choose a router role: **Border** or **Edge**.
Transport gateway	This option is available only when Multi-Region Fabric is enabled. Choose **Enabled** or **Disabled**.

4. This step is applicable only when you enable configuration groups.

Configure the device parameters:

The system IP address is not auto-populated for the interconnect connections. Click the edit icon for the chassis number to modify the following:

- **System IP**
- **Host name**
- **DNS Address (vpn_dns_primary)**
- **DNS Address (vpn_dns_secondary)**
- **Color**
- **Username**
- **User password**

Click **Next**.

5. Click **Deploy**.

When the configuration task is successful, the interconnect gateway is listed in the **Gateway Management** page.

Cloud Connections

VPC connectivity

In the Cloud OnRamp for Multicloud onboarding page, click **Add connections** and choose the provider. Alternatively, you can create connectivity by clicking **Edit** on the intent management page for the selected cloud provider from the **Cloud Connections** tab in the dashboard view.

When the system records your intent for connectivity, it maps the intent in regions where a cloud gateway is present. This means that the VPC is reachable for VPNs that have a green color status.You can enter mapping intents even if cloud gateways are not present in certain regions. The system preserves and realizes your mapping intent when it discovers a new cloud gateway or mapping change. As cloud gateways are instantiated in different regions, the system realizes the mapping intents in those regions. Similarly, tagging operations can influence the mapping in different regions, and the system realizes mappings according to the tags in the cloud.

The **Cloud Connections** page displays the connectivity status with the following legends:

- Blank - Editable
- Grey color - System Defined
- Blue color - Intent Defined

  Expressed intent between two tags or a VPN and a tag. Connectivity is not realized until a VPC in a tag and cloud gateway have regional overlap.

- Green color - Intent Realized

  All tagged VPCS/VNets have connectivity to a cloud gateway.

- Orange Color: Intent Partially Realized

A combination of blue and green. Not all regions with tagged VPCs/VNets have connectivity.

- Red color - Intent Realized With Errors

  Cisco Catalyst SD-WAN attempted connectivity but found errors.

Note Cisco Catalyst SD-WAN supports only those cloud connections that have regions where Cisco Catalyst 8000V deployed.

Cloud router connectivity

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

The cloud router connectivity tab is only available for cloud gateways that need connectivity to existing Transit Gateways.

From cloud router connectivity tab, you can manage connectivity between cloud gateways, and between Cisco Catalyst 8000V Transit VPCs and the Transit Gateway. The matrix displays the connectivity status between the VPNs and the cloud gateways (implicitly the Transit Gateways) they are attached to. Click any of the cells in the matrix displayed to get detailed information on the status.

Click **Edit** on cloud router connectivity page. Select any cell in the matrix and click **Add attachments** to update the routing table on the Transit Gateway that you want to connect to. Click **Save** on the routing table as well as the main matrix view to save the changes.

Once the Cisco Catalyst 8000V VPNs are connected to the Transit Gateway using VPN attachments over desired Transit Gateway route tables, to establish connectivity between Transit Gateway and VPC, see Configure Transit Gateway connections through AWS portal, on page 263.

Configure Transit Gateway connections through AWS portal

When you create an AWS cloud gateway, in the Transit Gateway field if you choose **Use Existing** or **Connect later/skip connection**, use this procedure to connect the cloud gateway to the Transit Gateways in the AWS portal.

Before you begin

Procedure

Step 1 Verify the VPN tunnel status.

a) From the AWS portal, click **Virtual Private Network (VPN)** > **Site-to-Site VPN connections** to navigate to the region in which the cloud gateway is created in Cisco SD-WAN Manager.

b) Select the VPN ID associated to the Transit Gateway ID and verify that the tunnel active.

Step 2 Create the Transit Gateway attachment.

a) Select the **Attachment Type** as **VPC** from the drop-down menu.

b) Select the VPC from the **VPC ID** drop-down list to attach the Transit gateway on Cisco SD-WAN Manager.

c) Click **Create the transit gateway attachment**.

Step 3 Create propagation with host VPC attachment in route table.

a) From the AWS portal, click **Virtual Private Cloud** > **Transit Gateways** > **Transit Gateway Route Table**.
b) Select the route table that was used to create the cloud gateway in Cisco SD-WAN Manager.
c) Select the propagation tab and click **Create propagation** to add the host VPC attachment.
d) Add the VPC attachment from Step 2 to the propagation. click on **Add Propagation**.
Verify the propagation is successful by checking the routes on selection of the route table.

Step 4 Create a new route table to associate the host VPC and propagate the VPN connections.

Step 5 Select the host VPC and **Add Route** by selecting routes through the Transit Gateway attachment to the main route table of the host VPC.

Rebalance VNets

You can choose to redistribute VNets to load balance the existing VNets among all the cloud gateways in a region for a given tag at any time. You can reassign only the VNets with **Auto** option selected across cloud gateways. The VNets assignment is based on a load-balancing algorithm. As the rebalancing involves detachment and re-attachments of VNETs to cloud gateways, traffic disruption may occur. After rebalancing the VNets, you can view the revised mapping of VNETs to cloud gateways on the tagging page.

Note You cannot rebalance VNets when:

- Create, edit, or delete of Cloud gateway is in progress.
- Mapping of VNets is in progress.
- Audit is in progress.

1. In **Cloud Connections** page, choose **Azure** or **Azure Gov Cloud** and click **Rebalance VNets**
2. In the **Region** field, choose a region from the drop-down list.
3. In the **Tag Name** field, choose a tag from the drop-down list.
4. Click **Save**.

Interconnect Connections

Interconnect connections that are created in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier releases are automatically mapped into the middle-mile netwroks, multicloud networks, and the virtual networks workflows.

The connection names of the multicloud networks and virtual networks are in the following format:

AWS:

- Private connections: AWS-<Name of DxGW> ::<UUID of DGW>
- Public connections: AWS_PUBLIC_CONNECTION::<Account ID>

Azure connections: AZURE-<ERC Name>-<Auth Key>

Google Cloud:

- Private connections: GCP <Region>::<Name of Google Cloud Route>r::<Name of Attachment>

Middle-Mile Networks

This section helps you create a middle-mile fabric between Interconnect gateways or a virtual connection from an Interconnect gateway to a cloud provider's on-ramp location.

Create Middle-Mile Networks to AWS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

Field	Description
Destination	From the drop-down list, choose **Cloud-AWS**.
Connection source	Choose an interconnect gateway from the drop-down list.
Cloud gateway connection	Enable to extend the SD-WAN fabric to a cloud gateway.

   Click **Next**.

3. **Connect to AWS**:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.
Cloud access type	Choose one of the following: • **Public Services** • **Private Workloads**

   If you choose **Public Services**:

Field	Description
Cross-connect type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Hosted VIF** A virtual interface (VIF) in AWS is a connection that allows access to AWS services. • **Hosted Connection** This is the default option if **Advanced layout** option is not enabled. **Note** Equinix only supports public, private, and transit VIFs over a hosted connection. Hosted VIFs are not supported.
VPN segment	Choose the segment ID for this connection.
Cloud OnRamp location	Select the AWS on-ramp connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Select or enter AWS account	Select an AWS account or enter an AWS account ID details to establish an interconnect connection.
Account ID	Enter the AWS account ID. This option is available only if you select **Enter AWS account ID** in the **Select or enter AWS account** field.
Interconnect IP address	Enter the source BGP peering subnet public IP address for the interconnect gateway.
Amazon IP address	Enter a public IP address for AWS BGP peer.
Prefixes to be advertised to AWS	Enter prefixes to advertise to AWS.
(Optional) **Source BGP ASN**	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. Enter an ASN supported by your provider.

If you choose **Private Workloads**:

Field	Description
Cross-connect type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Hosted VIF** • **Hosted Connection** This is the default option if **Advanced layout** option is not enabled.
Virtual network association type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Direct to VPC** • **Transit Gateway** This is the default option if **Advanced layout** option is not enabled.
VPN segment	Choose the segment ID for this connection.
Cloud OnRamp location	Select the AWS on-ramp connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Select or enter AWS account	Select an AWS account or enter an AWS account ID details to establish an interconnect connection.
Account ID	Enter the AWS account ID. This option is available only if you select **Enter AWS account ID** in the **Select or enter AWS account** field.
Direct connect gateway BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and direct connect gateway in your cloud provider. Check with you provider for the supported ranges.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP Peering IP** • **Destination BGP Peering IP** • **Source BGP ASN**

Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Middle-Mile Networks** page.

Create Middle-Mile Networks to Azure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

   :

Field	Description
Destination	From the drop-down list, choose **Cloud-Azure**. **Note** Make sure to create the necessary Express Route circuit in the appropriate region before proceeding. You can create these resources using the **Multicloud Networks** page or directly in the cloud provider.
Cloud gateway connection	Enable to extend the SD-WAN fabric to a cloud gateway.
Primary connection source	Choose a primary interconnect gateway from the drop-down list.
Secondary connection source	Choose a secondary interconnect gateway from the drop-down list.

   Click **Next**.

3. **Connect to Azure**:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.

Field	Description
Cloud access type	Choose one of the following: • **Microsoft Services** • **Private Workloads**

If you choose **Microsoft Services**:

Field	Description
VPN segment	Choose the segment ID for this connection.
Select account or enter express-route circuit	Select an Azure account or enter an express route circuit key.
Azure express-route circuit	Click on the refresh button to get the latest list from cloud provider. Select the Azure Express Route circuit from the drop-down list. This option is available only if you select **Enter an express-route circuit** in the **Select account or enter express-route circuit** field.
Primary cloud OnRamp location	The primary Azure connection location field is auto-populated based on the Azure Express Route circuit selection. You cannot modify this field.
Secondary cloud OnRamp location	The selection Azure connection location field is auto-populated based on the Azure Express Route circuit selection. You cannot modify this field.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Primary connection peering IP addresses	
Interconnect IP address	Enter the public IP Address to be used as the source BGP peering subnet ID for the interconnect gateway.
Azure IP address	Enter the public IP Address to be used as the destination BGP peering for the interconnect gateway.
Secondary connection peering IP addresses	
Interconnect IP address	Enter the public IP Address to be used as the source BGP peering subnet ID for the interconnect gateway.

Field	Description
Azure IP address	Enter the public IP Address to be used as the destination BGP peering for the interconnect gateway.
Prefixes to be advertised to Azure	Enter prefixes to advertise to Azure.
Source BGP ASN This field is available only if you enable **Advanced layout** option.	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

If you choose **Private Workloads**:

Field	Description
Virtual network association type This field is available only if you enable **Advanced layout** option.	Choose one of the following: • **Direct to VNets** • **Virtual WAN and vHubs** This is the default option if **Advanced layout** option is not enabled.
VPN segment	Choose the segment ID for this connection.
Select account or enter express-route circuit	Select an Azure account or enter an express route circuit key.
Azure express-route circuit	Click on the refresh button to get the latest list from cloud provider. Enter the details of Azure Express Route circuit. This option is available only if you select **Enter an express-route circuit** in the **Select account or enter express-route circuit** field.
Primary cloud OnRamp location	The primary Azure connection location field is auto-populated based on the Azure express route circuit selection. You cannot modify this field.
Secondary cloud OnRamp location	The secondary Azure connection location field is auto-populated based on the Azure express route circuit selection. You cannot modify this field.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

Field	Description
Connection peering settings This field is available only if you enable **Advanced layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Primary connection peering IP addresses** • **Interconnect IP address** • **Azure IP address** • **Secondary connection peering IP addresses** • **Interconnect IP address** • **Azure IP address** • **Source BGP ASN**

Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Middle-Mile Networks** page.

Create Middle-Mile Networks to Google Cloud

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.
2. Configure the intent:

Field	Description
Destination	From the drop-down list, choose **Cloud-Google**. **Note** Make sure to create the necessary Google Cloud router and Interconnect attachment in the appropriate region before proceeding. You can create these resources using the **Multicloud Networks** page or directly in the cloud provider.
Cloud gateway connection	Enable to extend the SD-WAN fabric to a cloud gateway. If you enable, enter the following details: • **Primary connection source** • **Secondary connection source**
Redundancy	Choose **Enable** if you want to create connections with redundancy. Enter the following details: • **Primary connection source** • **Secondary connection source** Choose **Disable** if you want to create the connection without redundancy. Enter the following details: • **Connection Source**

Click **Next**.

3. Configure a connection to Google Cloud:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.
VPN segment	Choose the segment ID for this connection.
Select account or enter pairing key for attachment	Select an account or enter a pairing key for the attachment.

If you choose to select an account when redundancy is enabled:

Field	Description
Google region	Choose a Google Cloud connection location.
VPC network	Choose the VPC network to deploy this connection.
Primary Connection	

Field	Description
Cloud router	• Click the refresh symbol next to the **Cloud Router** drop-down list. • Choose a Google Cloud router.
Google interconnect attachment	Choose the desired interconnect attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Secondary Connection	
Cloud router	• Click the refresh symbol next to the **Cloud Router** drop-down list. • Choose a Google Cloud router.
Google interconnect attachment	Choose the desired interconnect attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you choose to select an account when redundancy is disabled:

Field	Description
Google region	Choose a Google Cloud connection location.
VPC network	Choose the VPC network to deploy this connection.
Connection	
Cloud router	• Click the refresh symbol next to the **Cloud Router** drop-down list. • Choose a Google Cloud router.

Field	Description
Google interconnect attachment	Choose the desired interconnect attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you choose to enter a pairing key for the attachment when redundancy is enabled:

Field	Description
Primary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Secondary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you choose to enter a pairing key for the attachment when redundancy is disabled:

Field	Description
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

If you enable cloud gateway connection to extend the SD-WAN fabric to a cloud gateway through the middle-mile networks.

Field	Description
Connection name	Enter a unique name for the connection.
Select account or enter pairing key for attachment	Select an account or enter a pairing key for the attachment.
Google Cloud Gateway	Choose the Google Cloud gateway you wish to attach to this connection.
Primary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Secondary connection	
Google interconnect attachment	Enter a pairing key for the attachment.
Cloud OnRamp location	Choose a Google Cloud connection location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

Field	Description
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source BGP ASN**

Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

   When you save the connection configuration, a configuration task is launched and creates the interconnects between the Interconnect Gateway and the interconnect attachments of the Google Cloud routers.

   When the task is successful, the connections are listed on the **Middle-Mile Networks** page. You can also view the connection details on the Google Cloud console.

When you connect an Interconnect gateway to Google Cloud using Middle-Mile Networks, Cisco SD-WAN Manager does not automatically set up the connection. The connection is set up in Multicloud Networks.

However, since a pairing key based connection is not applicable to Multicloud Networks, you have to set up the connection manually. Perform the following steps in your Google Cloud environment:

1. Activate and set up the Autonomous System Number (ASN) for the Interconnect attachment. This number identifies your network to Google Cloud.
2. Get the Cloud Router's IP address and the peer BGP IP address. These addresses are needed for routing traffic.
3. Set up a VRF instance. This keeps the routing information of the connection separate.
4. Configure the VRF BGP settings under the Interconnect Gateway using the appropriate interface. This enables your network and Google Cloud to share routing information.

Create Interconnect Between Interconnect Gateways

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Middle-Mile Networks**.

2. Configure the intent:

Field	Description
Destination	From the drop-down list, choose **Device Connect**.
Connection source	Select an interconnect gateway from the drop-down list.

Click **Next**.

3. Configure the device connections:

   To view available Interconnect Connection licenses associated with the account, click **View license**.

Field	Description
Connection name	Enter a unique name for the connection.
Connection destination	Choose a destination interconnect gateway.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Connection peering settings This field is available only if you enable **Advanced Layout** option.	Choose one of the following for BGP settings: • **Autogenerated** This is the default option if **Advanced layout** option is not enabled. • **Custom** If you choose **Custom**, enter the following: • **Source IP Address and Prefix** • **Destination IP Address and Prefix**

   Click **Next**.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Middle-Mile Networks** page.

Device Links

Device link groups create a full-mesh network between two or more edge devices. Device links connects all the edge devices, that are part of a group, together to create a WAN. All the device links in a mesh share the same bandwidth between the edge devices.

Note

- Only one device link is supported per Equinix account.
- Point to point connection cannot be formed between interconnect gateways belonging to a device link group.

Add Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Click **Middle-Mile Networks**.
4. Select **Device Links**.
5. Click **Add Device Link**.
6. Configure the following parameters:

Field	Description
Account name	Choose an account from the drop down menu. This is the Equinix account that has been associated to Cisco SD-WAN Manager through Account Association.
Device link name	Enter a name for the device link.
Bandwidth	Choose the bandwidth from the drop down menu. **Note** The maximum bandwidth supported by Equinix is 10000 Mbps per metro.
Subnet (Optional)	Enter the subnet. **Note** • Provide IP subnets for interconnect gateway device link interface. • The subnet should be in 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 range. • The subnet should not conflict with 172.31.251.0/21. • The subnet should not conflict with other connections. • If you do not enter the subnet, 198.19.0.0/16 is used by default.

Field	Description
Gateway name	Select the gateways from the drop down menu. Select at least two gateway names.

7. Click **Next** to preview the summary.
   - To create the device link, click **Submit**.
   - To modify the parameters, click **Back**.

Update Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Click **Middle-Mile Networks**.
4. Click **Device Links**.
5. Existing device links are summarized in a table.
6. In the table, find the desired link and click **...**.
7. To edit the device link, click **Edit**.
8. In the **Edit Device Link** page, you can only update the **Bandwidth** and **Gateway Name** to add or remove gateways.



Note Bandwidth and Gateway Name are the only two parameter that can be edited.

When adding or removing devices, at least two devices should be present in the device link.

The maximum bandwidth supported by Equinix is 10000 Mbps per metro.

9. Click **Save**.

Delete Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Click **Middle-Mile Networks**.
4. Click **Device Links**.
5. Existing device links are summarized in a table.
6. In the table, find the desired link and click **...**.
7. To delete a device link, click **Delete** and confirm that you wish to delete the device link.

Multicloud Networks

This section helps you create cloud network resources, such as Direct Connect Gateways, ExpressRoute Circuits, or Google Cloud Routers. These resources are essential for connecting middle-mile network connections to your cloud workloads (VPCs/VNets).

Ensure that both Cloud Gateways and Interconnect Gateways use the same configuration method, either templates or configuration groups.

Create Multicloud Networks to AWS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Multicloud Networks**.

2. Configure the cloud intent:

Field	Description
Cloud type	From the drop-down list, choose **AWS**.
Cloud access type	Choose one of the following: • **Public services** • **Private workloads**

3. If you choose **Public services** make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Direct connect gateway account	Choose a direct connect gateway account from the drop-down list.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose the middle-mile network connection from the drop-down list. Only middle-mile network connections matching the direct gateway's BGP ASN are displayed in the drop-down list.

   If you choose **Private workloads** make the following configurations:

Field	Description
Virtual network association type This field is available only if you enable **Advanced Layout** option.	Choose one of the following: • **Direct to VPC** • **Transit gateway** This is the default option if **Advanced layout** option is not enabled. • **Cloud gateway connection**

Field	Description
Connection name	Enter a unique name for the connection.
Direct connect gateway account	Choose a direct connect gateway account from the drop-down list.
Direct connect gateway	Click on the refresh button first. Choose a direct connect gateway from the drop-down list. Alternatively, create a new **Direct Connect Gateway** by clicking **Create New**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**. From Cisco Catalyst SD-WAN Manager Release 20.16.1, AWS Direct Connect Gateways are shared only by connections having the same virtual network association type (Direct to VPC, Transit Gateway or Cloud Gateway). When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.16.1 or later releases, ensure that the AWS Cloud Gateway connections and Private VPC connections do not share the same Direct Connect Gateway. Delete any connections that share the same Direct Connect Gateway if they are not of the same virtual network connection type.
Connectivity configuration	• **Interconnect attachments** • **Gateway Associations** This option is applicable to virtual network association type **Transit Gateway** and **Cloud gateway connection**.
If you choose **Interconnect attachments**:	

Field	Description
Middle-mile network connections	Choose the middle-mile network connection from the drop-down list. Only middle-mile network connections matching the direct gateway's BGP ASN which are of the same type as current multicloud networks connection are displayed in the drop-down list.
If you choose **Gateway Associations** and if you choose **Cloud gateway connection**:	
+ AWS region(s)	Click to add AWS regions.
AWS region	Select the AWS on-ramp connection location.
Cloud gateway	Click on the refresh button first. Choose a cloud gateway for the selected region from the drop-down list.
If you choose **Transit gateway**	
+ AWS region(s)	Click to add AWS regions.
AWS region	Select the AWS on-ramp connection location.
Transit gateway	Click on the refresh button first. Select transit gateway associated to the AWS account. Alternatively, create a new **Transit gateway** by clicking **Add New**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.
Prefixes	Enter the IPv4 prefixes for the selected gateway.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Multicloud Networks** page.

Create Multicloud Networks to Azure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Multicloud Networks**.

2. Configure the cloud intent:

Field	Description
Cloud type	From the drop-down list, choose **Azure**.
Cloud access type	Choose one of the following: • **Microsoft services** • **Private workloads**

3. If you choose **Microsoft services** make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Express route circuit account	Choose an Azure account from the drop-down list to establish an interconnect connection.
Express route circuit	Click on the refresh button first. Choose an express route to attach an interconnect connection or click **Add New**. If you clicked **Add New**, configure the express route settings and click **Save**: • **Resource Group**: Choose a resource group associated with the Microsoft Azure account. • **Region**: Choose an Azure region. • **Instance Name**: Enter a name for the ExpressRoute instance. • **Provider**: Choose Megaport. • **Peering Location**: Choose an ExpressRoute location. • **Bandwidth**: Choose the bandwidth of the ExpressRoute circuit. • **SKU**: Choose the **Premium** or the **Standard** SKU. • **Billing Model**: Choose **Metered** billing or **Unlimited**.
Connectivity configurations	Choose **Interconnect attachments**.
Middle-mile network connections	Choose the interconnect circuits from the drop-down list. Only middle-mile network connections that are applicable are displayed in the drop-down list.

If you choose **Private workloads** make the following configurations:

Field	Description
Virtual network association type This field is available only if you enable **Advanced Layout** option.	Choose one of the following: • **Direct to VNets** • **Virtual WAN** This is the default option if **Advanced layout** option is not enabled. • **Cloud gateway connection**

Field	Description
Connection name	Enter a unique name for the connection.
Express route circuit account	Choose an Azure account from the drop-down list to establish an interconnect connection.
Express route circuit	Click on the refresh button first. Choose an express route to attach an interconnect connection or click **Add New**. If you clicked **Add New**, configure the express route settings and click **Save**: • **Resource Group**: Choose a resource group associated with the Microsoft Azure account. • **Region**: Choose an Azure region. • **Instance Name**: Enter a name for the ExpressRoute instance. • **Provider**: Choose Megaport. • **Peering Location**: Choose an ExpressRoute location. • **Bandwidth**: Choose the bandwidth of the ExpressRoute circuit. • **SKU**: Choose the **Premium** or the **Standard** SKU. • **Billing Model**: Choose **Metered** billing or **Unlimited**.
Connectivity configurations	Choose one of the following: • **Interconnect attachments** • **Gateway Associations**

Field	Description
Middle-mile network connections	Choose the interconnect circuits from the drop-down list. Only middle-mile network connections that are applicable are displayed in the drop-down list.
If you choose **Gateway Associations**:	
Azure virtual WAN This field is available only if you enable **Advanced Layout** option and choose **Virtual WAN**.	Choose or add a new virtual WAN.
+ Add virtual hub(s)	Click to add Azure virtual hubs.
Azure region	Select the Azure connection location.
Virtual hub	Click on the refresh button first. Choose a virtual hub for the selected region from the drop-down list.
These fields are available only if you enable **Advanced Layout** option and choose **Cloud gateway connection**.	
+ Add Cloud Gateways	Click to add cloud gateways.
Azure region	Select the Azure connection location.
Cloud gateway	Click on the refresh button first. Choose a cloud gateway for the selected region from the drop-down list.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Multicloud Networks** page.

Create Multicloud Networks to Google Cloud

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Multicloud Networks**.

2. Configure the cloud intent:

Field	Description
Cloud type	From the drop-down list, choose **Google Cloud**.

Field	Description
Virtual network association type	Choose one of the following: • **Shared VPC** • **Cloud gateway connections**
Redundancy	Choose **Enable** if you want to create connections with redundancy. Choose **Disable** if you want to create the connection without redundancy.

3. If you choose **Shared VPC** and **Enable** redundancy make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Google account	Choose a Google Cloud account to establish an interconnect connection from the drop-down list.
Google region	Select the Google Cloud connection location.
VPC network	Choose the VPC network to deploy this connection.
Primary Google Cloud router	Select a primary Google Cloud router or create a new one for the partner interconnect connection. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Google Cloud Router: Enter a unique Google Cloud router name.

Field	Description
Primary Google Cloud interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Secondary Google Cloud router	Select a secondary Google Cloud router or create a new one for the partner interconnect connection. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Google Cloud Router: Enter a unique Google Cloud router name.

Field	Description
Secondary Google Cloud interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose a middle-mile network connections to connect to the Google Cloud.

If you choose **Shared VPC** and **Disable** redundancy make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.
Google account	Choose a Google account to establish an interconnect connection from the drop-down list.
Google region	Select the Google cloud connection location.
VPC network	Choose the VPC network to deploy this connection.

Field	Description
Google cloud router	Select a Google Cloud router or create a new one for the partner interconnect connection. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Google Cloud Router: Enter a unique Google Cloud router name.
Google interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose a middle-mile network connections to connect to the Google Cloud.

If you choose **Cloud gateway connections** make the following connectivity configurations:

Field	Description
Connection name	Enter a unique name for the connection.

Field	Description
Google account	Choose a Google Cloud account to establish an interconnect connection from the drop-down list.
Google Cloud gateway	Choose the Google Cloud gateway you wish to attach to this connection.
Primary Google Cloud router	This field is auto-populated based on the selection of the Google Cloud gateway. You cannot modify this field.
Primary Google interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Secondary Google Cloud router (Optional)	This field is auto-populated based on the selection of the Google Cloud gateway. You cannot modify this field.

Field	Description
Secondary Google interconnect attachment	Choose the desired interconnect attachment or click **Add New**. If you clicked **Add New**, configure the router settings in the slide-in pane. Configure the following and click Save: • **Region**: Choose the Google Cloud Interconnect attachment region. • **VPC Network**: Choose the Google Cloud network for the interconnect attachment. • **Cloud Router Name**: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • **Google Cloud Router Interconnect Attachment Name**: Enter a unique name for the interconnect attachment. • **Secondary Zone**: If you want to deploy this attachment on the secondary zone, check the checkbox.
Connectivity configuration	Choose **Interconnect attachments**.
Middle-mile network connections	Choose a middle-mile network connections to connect to the Google Cloud.

4. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Multicloud Networks** page.

Virtual Networks

This section helps you to associate multicloud network connections with your cloud workloads (VPCs/VNets).

Create Virtual Networks to AWS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Virtual Networks**.
2. Configure cloud infrastructure connectivity:

Field	Description
Connection name	Enter a unique name for the connection.
Cloud	Select AWS as the cloud provider.
Cloud account	Select an AWS account from the drop-down list.
Virtual Network Tag Association	
Virtual network tag(s)	Choose VPC tags to identify VPCs for which traffic must be routed through this connection. See Create Tags for AWS, on page 241.
Multicloud network connection	Choose a multicloud network connection.

Click **Next**.

3. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Virtual Networks** page.

Create Virtual Networks to Microsoft Azure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

   From the onboarding page, click **Add connections** and choose the provider.

   Alternatively, click **Add connections** from the **Interconnect Connections** tab in the dashboard view.

   Select **Virtual Networks**.

2. Configure cloud infrastructure connectivity:

Field	Description
Connection name	Enter a unique name for the connection.
Cloud	Select Azure as the cloud provider.
Cloud account	Select an Azure account from the drop-down list.
Virtual Network Tag Association	
Virtual network tag(s)	Choose VNet tags to identify VNets for which traffic must be routed through this connection. See, Create Tags for Azure and Azure Gov Cloud , on page 242.
Multicloud network connection	Choose a multicloud network connection.

Click **Next**.

3. Review the connection summary.
   - To create the connection, click **Deploy**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Virtual Networks** page.

View, Edit, or Delete Connections

View Connection Properties

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Based on your requirements, click **Middle-Mile Networks**, **Multicloud Networks**, or **Virtual Networks**.

   Existing connections are summarized in a table.
4. To view more information about a connection, click **...** for the desired connection and click **View**.

Edit Connection Configuration

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Based on your requirements, click **Middle-Mile Networks**, **Multicloud Networks**, or **Virtual Networks**.

   Existing connections are summarized in a table.
4. To modify connection configuration, click **...** for the desired connection and click **Edit**.

   Along with these editable parameters, Cisco SD-WAN Manager also displays read-only properties about the connection.

Note You can modify the properties of active connections only.

5. To apply the changes, click **Update** or **Save**.

Delete Connection

Note

- When you delete a connection to AWS, Cisco SD-WAN Manager deletes only the VIF, the virtual private gateway, and the route table that were created while establishing the connection.

  To delete cloud resources created during AWS virtual interface connection:

  1. Edit the Multicloud networks connection and delete the attachment.
  2. Delete the correspondent middle-mile networks connection to detach the cross connect.
  3. Delete the Multicloud networks connection.

- While creating a connection to AWS, if you created a direct connect gateway or a transit gateway, you can optionally delete the direct connect gateway and transit gateway.
- When you delete a connection to Azure, Cisco SD-WAN Manager deletes any ExpressRoutes, VNet gateways, ExpressRoute gateways, and virtual hubs created for the connection only if these elements are not used in other connections. Azure Virtual WAN cannot be deleted when you delete a connection.

  When you delete a GCP connection, you can optionally select to delete the Google Cloud Router, or manage these resources as required.
- Express-routes cannot be deleted until they are detached from the middle-mile cross connection. If you want to delete an express-route:
  1. Edit the multicloud metworks connection and delete both the primary and secondary attachments.
  2. Delete the correspondent middle-mile networks connection to detach the cross connect from the express-route.
  3. Delete the multicloud networks connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect Connections**.
3. Based on your requirements, click **Middle-Mile Networks**, **Multicloud Networks**, or **Virtual Networks**.

   Existing connections are summarized in a table.
4. To delete a connection, click **...** for the desired connection and click **Delete**. Confirm that you wish to delete the connection.

Audit

This is a user-invoked audit. Follow these steps to initiate an on-demand audit:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the dashboard page, click **Audit**.
3. Perform one of the following:
   - Select the public cloud provider and click **Run audit**

- or, select the interconnect providers, choose **Interconnect Connections**, **Destination type**, and **Cloud Provider**, and click **Submit**.

  When you choose Equinix you can also choose **Device links** for audit.

The window displays the status for various instances. If the status is **In Sync** for any of the objects, it means the object is free from errors. If the status of an object is **Out of Sync**, it means that there are discrepancies between the instance details available on Cisco SD-WAN Manager and the details available on the provider database.

4. If the status of an instance shows **Out of Sync**, it means that it is an error that requires manual intervention or a review and rerun of the audit to fix the error.



Note The multicloud audit service does not run while other cloud operations are in progress.

AWS audit-reported anomalies and fixes

Table 59: Examples of AWS audit discrepancies

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Transit Gateway Attachment with Resource Type as **VPC** in AWS (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details**: Mapping issue Connectivity element was missing from response: [srcType:VPC ID dstType: <C8kv-device1-UUID]> Connectivity element was missing from response: [srcType: <C8kv-device1-UUID >dstType: VPCID]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the applicable solution type.
Missing site-to-site VPN Attachment (Transit Gateway Attachment Type VPN) in AWS	Transit Gateway–VPN based (using TVPC) / Cloud WAN–VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: Mapping **Details**: Mapping issue vpnAttachSpec with tunnelId: <C8kv-device1-UUID >:<VPNID> was missing from the cloud.	Yes, audit-fix workflow - 1 is triggered.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Transit Gateway Attachment > VPC Attachment in secondary AWS account (Applicable when CGW and workload hosts are in different accounts) (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:VPC src: VPC1-Account1 dstType: VPC2 dst: VPC2] Connectivity element was missing from response: [srcType:VPC src: vpc-1 dstType: <C8kv-device1-UUID>]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the solution type.
Missing Transit Gateway Attachment with resource type as **Connect** in AWS	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC)	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:<C8kv-device1-UUID> dstType:VPC dst:VPCID] Connectivity element was missing from response: [srcType: C8kv-device2-UUID> dstType:VPC dst:VPCID]	Yes, audit-fix workflow - 2 is triggered.
Missing Host VPC (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: HOSTVPC **Details:** Host Vpc issue: <VPC ID> Hostvpc: <VPC ID> Tag mismatch- [<TAG NAME>! =] Hostvpc: <VPC ID> Couldn't find in the cloud.	Yes, audit will remove the missing VPC from tag(s) and from discovered VPC list.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing TGW	Transit Gateway–VPN based (using TVPC) / Cloud WAN VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TGW **Details:** Cloud Gateway (TGW) issue: TGW missing from the cloud. Name: <TGW Name>, region: <Region>. Please recreate the Cloud Gateway	Not fixable
Missing C8kv	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC) / Transit Gateway–VPN based (using TVPC) / Cloud WAN – VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TVPC **Details:** Cloud Gateway (TVPC) issue. Name: <CGW Name>, Id:<TVPC Id>. Please recreate the Cloud Gateway.	Not fixable
Invalid credentials	All	Could not perform audit at this time. Please retry after 10 minutes. Audit Failure.	Not fixable

Note Network connectivity disturbance is expected when the audit-fix (on-demand or periodic) is in progress, as the fix workflow deletes and recreates attachments and mappings in all the regions.

Note VPCs referred to are those discovered and tagged by Cisco SD-WAN Manager. “Missing” is defined in the context of the Cisco SD-WAN Manager’s database/knowledge.

Note Audit-fix performs the same steps in both on-demand (that is, clicking the **Fix Sync Issues** button) and periodic audit scenarios.

Note Audit-fix deletes all out-of-band attachments (VPC, TGW-peering, and Connect) to TGW or CloudWAN that users have manually created or mapped outside of CoR workflow, if any exist.

Azure audit-reported anomalies and resolutions

Table 60: Examples of Azure audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
If the VNet is tagged in the Cisco SD-WAN Manager database, but it is not available in the Azure portal.	**Report Type**: VNet and Mapping **Details**: **VNet issue**: Cloud Virtual Network Issue: Not Found on Azure portal Name: <vnet-name>. Error received from Azure: Azure Error: ResourceNotFound Message: The resource '<vnet-name>' under resource group '<rg-name>' was not found. For more details, see https://aka.ms/ARMResourceNotFoundFix **Mapping issue**: Virtual Hub is mapped with virtual network <vnet-name> that does not exist.	The audit will remove the mapping from Cisco SD-WAN Manager. The audit will remove VNet from Cisco SD-WAN Manager.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
If the VNet tag is removed from the Azure portal, or if a VNet tag mismatch exists between Cisco SD-WAN Manager and Azure portal.	**Report Type**: VNet **Details**: Cloud Virtual Network Issue: Tag On Cisco SD-WAN Manager is not the same as Azure portal Name: <vnet-name>.	Virtual network <vnet-name> will be tagged with <tag-name>.	Virtual network <vnet-name> will be tagged with <tag-name>.

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
If the storage account is not available in the Azure portal but it is available in the Cisco SD-WAN Manager database.	**Report Type**: Storage **Details**: Cloud Gateway (Storage) issue: Not Found on Azure Portal.Name: <name>, Id: <id>. A storage account is required to configure bootstrap for NVA create or edit operations. Error received from Azure: Azure Error: ResourceNotFound Message: The resource '<storage-account-name>' under resource group '<rg-name>' was not found. For more details please go to https://aka.ms/ARMResourceNotFoundFix	Storage account <storage-account-name> will be removed from Cisco SD-WAN Manager.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
If virtual WAN, vHub, or NVA is not available in the Azure portal.	**Report Type**: VWAN, vHub, NVA, Mapping	Audit removes virtual WAN, vHub, NVA, mapping from the Cisco SD-WAN Manager database. **Note**: Do not delete the cloud gateway manually. Deleting the cloud gateway results in a discrepancy between the cloud providers and can impact the ability to provision anything further or impact other CoR operations.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
Mapping is found in the Cisco SD-WAN Manager database but it is not found in the Azure portal.	**Report Type**: Mapping **Details**: Mapping issue: Cloud Virtual Networks to Virtual Hub mapping issue. Mapping not found on Azure Portal with vNet <vnet-name>	Run audit-fix-sync issues to add virtual hub mapping to the Azure portal.	Audit adds virtual hub mapping to the Azure portal.

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
Mapping is found in the Azure portal, but it is not found in theCisco SD-WAN Manager database.	Audit shows in sync	Audit reports are in sync. To add the mapping back to the Cisco SD-WAN Manager database, add tag manually and map VNet using the Cisco SD-WAN Manager workflow.	Periodic audit reports are in sync. To add the mapping back to the Cisco SD-WAN Manager database, add tag manually and map VNet using the Cisco SD-WAN Manager workflow.
Account credentials expired	**Report Type**: VWAN, vHub, NVA, Mapping	You are required to manually update the account credentials.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You are required to manually update the account credentials.

Note Audit support for Azure was introduced in Cisco vManage Release 20.7.1.

Note Audit is not applicable for SD-Routing CoR (vHub with VPN) only deployment.

GCP audit-reported anomalies and fixes

Table 61: Examples of GCP audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message
Missing Network Connectivity Center (NCC) spokes	**Report Type**: NCC_HUB **Details**: Spoke <spoke-name> in region <region-id> is missing.
Missing NCC Hubs	**Report Type:** NCC_HUB **Details:** NCC Hub: <Hub Name> not found.
Missing Google cloud routers (GCRs) - primary, secondary, or both	**Report Type:** GCR **Details**: <GCR Name> not found.

Anomaly / Trigger	Audit Findings / Error Message
Missing site-to-cloud peering of VPCs mapped to VPNs in Cisco SD-WAN Manager	**Report Type**: MAPPING **Details**: Connectivity element was missing from response: [srcType:V dstType:VPC dst:<dst-vpc-id>]
Missing VPC peering of VPCs that are mapped to other VPCs in Cisco SD-WAN Manager	**Report Type:** MAPPING **Details:** Connectivity element was missing from response: [srcType: dstType:VPC dst:<dst-vpc-id>]
Missing custom routes	**Report Type:** Mapping **Details:** Connectivity element was missing from response: [srcType: src:<C8Kv-Device-UUID>::<vpn-id> dstType:VPC dst:<vpc-id>]
Missing Border Gateway protocol (BGP) sessions	**Report Type**: MAPPING **Details**: BGP session is missing in GCR
Stale BGP sessions	**Report Type**: MAPPING **Details**: Stale prefixes found in BGP Sessions
Removal of a cloud gateway or any of its components	**Report Type:** CGW_ROUTER **Details:** CGW Router: [<CGW Instance name> <region-id>] Couldr cloud (Irrecoverable error, user intervention needed to fix things in c
Issues with host VPCs with overlapping CIDRs	**Mapping Failure**: Additional details: Overlapping subnets part of ma Mapping: VPN:<vpn id> --> <s2c vpc name, vpc-id, vpc-subnet> / <vp **Report Type**: Mapping **Details**: vpnAttachSpec with tunnelId: <c8kv uuid>::<vpn id> was n
Issues with site-to-site VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2S_VPC] not found in cloud (Irrecove needed to fix things in cloud).
Issues with site-to-cloud VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2C_VPC] not found in cloud (Irrecove needed to fix things in cloud).
Issues with WAN VPCs	**Report Type:** TVPC **Details:**TVPC: [<s2c-vpc-id> WAN_VPC] not found in cloud (Irrecove needed to fix things in cloud).
Invalid GCP Credentials	**Report Type:** Account **Details:** Invalid GCP Credentials found for account Id <acc-id>

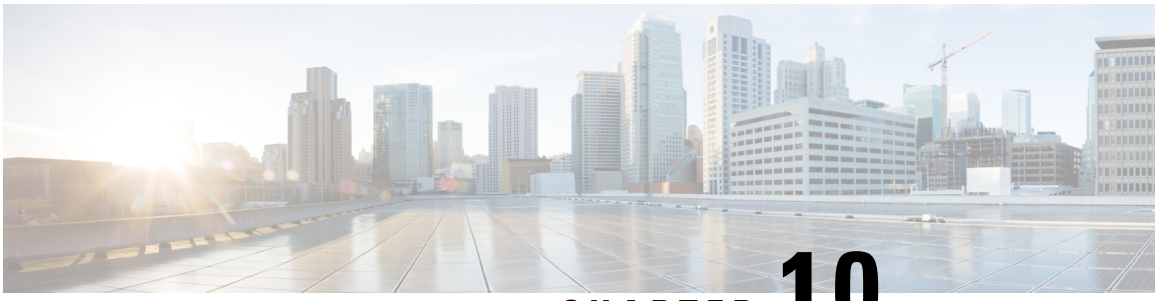
Note Audit-fix performs the same steps in both on-demand fix (that is, clicking the **Fix Sync Issues** button) and periodic audit followed by auto-correct.



PART III

Cloud OnRamp for Multicloud (Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Earlier)

- Cloud OnRamp for Multicloud, on page 305
- AWS Integration, on page 307
- Amazon GovCloud (US) Integration, on page 337
- Microsoft Azure Virtual WAN Integration, on page 343
- Microsoft Azure for US Government Integration, on page 375
- Google Cloud Integration, on page 379
- Cisco Catalyst SD-WAN Manager Support for Monitoring Multicloud Services, on page 401

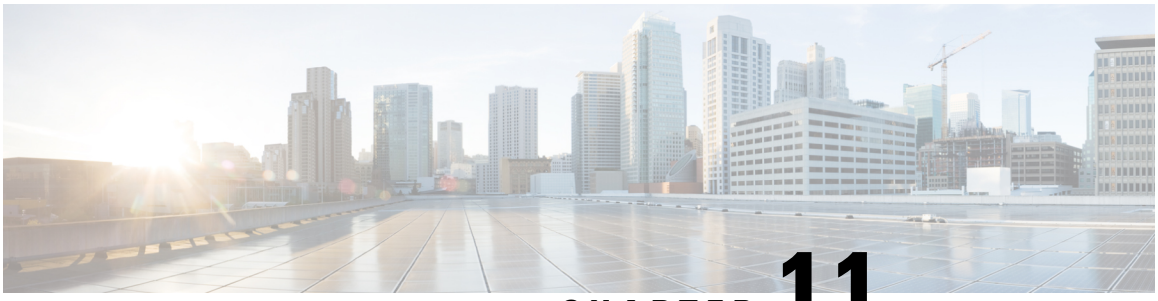


CHAPTER 10

Cloud OnRamp for Multicloud

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into the Cisco Catalyst SD-WAN fabric.

- AWS Integration, on page 307
- Microsoft Azure Virtual WAN Integration, on page 343
- Google Cloud Integration, on page 379
- Cisco Catalyst SD-WAN Manager Support for Monitoring Multicloud Services, on page 401



CHAPTER 11

AWS Integration

Table 62: Feature History

Feature Name	Release Information	Description
Integration of AWS Branch with Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	Cisco Catalyst SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into Cisco Catalyst SD-WAN fabric. This feature enables Transit Gateway when the standard Cloud OnRamp solution is not sufficient. For example, one host VPC is connected to the Cisco Catalyst SD-WAN edge router using an Internet Gateway. If the internet gateway bandwidth limit is less, then transit gateway is used for SD-WAN integration. It provides a way to interconnect VPCs and VPNs.
Support for Pay As You Go License for Cisco Catalyst 8000V Edge Software Instances	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	Cisco Catalyst 8000V Edge Software instances can be used with pay as you go (PAYG) licenses when creating a new cloud gateway in Amazon Web Services (AWS), in addition to the previously supported bring your own license (BYOL) model.
Integration of Cisco Catalyst SD-WAN Branches with AWS using Cisco IOS XE Catalyst SD-WAN Devices and the AWS Transit Gateway Connect feature	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This release enables the use of the AWS Transit Gateway Connect feature to connect a cloud gateway to an AWS transit gateway. This GRE based connection type offers improved bandwidth, scaling, and security compared to the use of IPSec VPN tunnel connections.

Feature Name	Release Information	Description
AWS Branch Connect Solution	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature leverages the AWS Transit Gateway support to connect branch devices to the cloud. The branch devices connect to transit gateway using an IPSec tunnel-based secure channel to access the applications hosted in the cloud. This feature supports scenarios where Cisco SD-WAN Manager instantiates, manages, and controls the AWS Transit Gateway.
AWS Cloud WAN Integration	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enables the use of AWS Cloud WAN to easily connect and route traffic from remote sites, regions and cloud applications over the AWS global network. This feature uses static routing for site-to-site communication.
AWS Cloud WAN Integration with Dynamic Routing	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature is an enhancement to the AWS Cloud WAN integration to support site-to-site communication using dynamic routing, leveraging AWS tunnel-less connect attachment.
Configure Devices for AWS Integration Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for AWS integration.

- Information about AWS Integration, on page 308
- Restrictions for AWS Integration, on page 313
- Configure AWS Integration, on page 314
- Intent Management - Connectivity, on page 328
- Transit Gateway Peering, on page 331
- Audit Management, on page 331
- Monitor AWS Integration using Cisco SD-WAN Manager, on page 335

Information about AWS Integration

A transit gateway is a network transit hub that you can use to interconnect your VPC and on-premises networks. You can attach a VPC, or a VPN connection to a transit gateway. It acts as a virtual router for traffic flowing between your VPC and VPN connections.

You can configure and manage Cloud OnRamp for Multicloud environments through the Cisco SD-WAN Manager controller. A configuration wizard in Cisco SD-WAN Manager automates the bring-up of the transit gateway to your public cloud account, the creation of cloud gateways that includes transit gateways and Cisco

Catalyst 8000V Edge, and the connections between public-cloud applications and the users of those applications at branches in the overlay network. This feature works with AWS virtual private clouds (VPCs) on Cisco cloud routers.

Cloud OnRamp for Multicloud supports integration with multiple AWS accounts. See Limitations for AWS Integration for details.

Supported Platforms

Cloud OnRamp for Multicloud on AWS supports the following platforms:

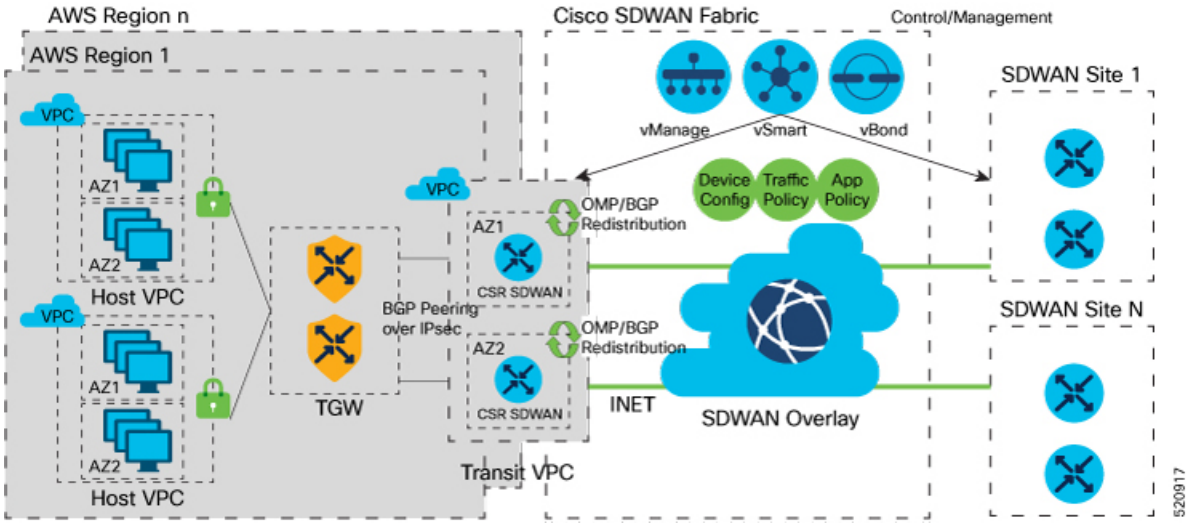
- Cisco Cloud Services Router 1000V Series (Cisco CSR1000V)

Note This platform is supported by Cisco SD-WAN Manager Release 20.3.x.

- Cisco Catalyst 8000V Edge Software

Note This platform is supported by Cisco SD-WAN Manager Release 20.4.x and later.

Architecture



Multicloud Dashboard

Multicloud dashboard in Cisco SD-WAN Manager consists of the following workflows:

- Setup
- Discover
- Manage
- Intent Management

Setup

You can create and manage cloud accounts and configure global settings in Cisco SD-WAN Manager for AWS automation. You can create multiple accounts, pick a specific account for transit gateway, mark one or more accounts for transit VPC automation and use other accounts for host VPC discovery and connectivity.

The multicloud dashboard supports **AWS key** and **IAM role** models for authentication. IAM roles only work for AWS cloud deployed Cisco SD-WAN Manager, as this requires special AWS AssumeRole functions. AssumeRole is used for cross-account access.

Global Settings

Global settings enables you to set a configuration one time and repeat across regions and handle resource management globally (per cloud). The software image and instance size specified are used for instantiation of CSRs in the cloud as part of the cloud gateway.

Global settings include:

- Software image: CSR software image used for creating cloud gateway.
- AWS Instance Size: CSR instance size used depending upon bandwidth requirements.
- Cloud Gateway Solution: The gateway solution used for AWS cloud. For example, transit gateway with transit VPC.
- IP subnet pool: IP subnet pool used for transit VPC creation across regions. Subnet pool can be customized per cloud gateway using custom settings option, if desired.
- Intra-Tag Communication: Allows or denies communication between the VPCs under the same tag.
- Default Route in Host VPCs: Default routes are automatically added to the main route table of the VPC that points to the transit gateway.
- Full Mesh of Transit VPCs: Setup a full mesh connectivity between TVPCs of cloud gateways in different regions so as to carry site to site traffic (through CSRs) over public cloud backbone.

Note When full mesh of transit VPCs is enabled in the global setting for Cisco Catalyst 8000V in an AWS deployment, the GigabitEthernet3 interface is automatically used for the configurations. This interface cannot be used for anything else, nor can the configuration of the interface be modified.

Note The image and the instance size selected once for global settings are not applicable to all the regions. The accounts used for the image discovery can be different and the selected image or the instance size may not be supported in all the regions. AWS instance size and the software image parameters can be changed only for the new cloud gateways that are created after the settings are updated.

For site-to-site communication, an additional interface is configured. The required configuration gets pushed or removed automatically when the site-to-site communication is enabled or disabled respectively in the global settings.

Discover VPCs

You can discover all the VPCs in all the accounts provided across regions. You can tag and untag these VPCs and use it for future connectivity. Cisco SD-WAN Manager creates tag with the key **Cisco-SDWAN-key** and you can customize the tag value for all VPCs within the same tag. The same tag can be used to map VPCs (that is, establish connectivity between VPCs) if the **Intra-Tag communication** in global settings is enabled. You can edit tags and change the membership of a tag associated with a VPC.



Note If you add a tag that is associated with an interconnect gateway, you cannot map it to an AWS cloud gateway in **Intent Management**.

Cloud Gateway

Cloud gateway comprises of a transit VPC, two CSR devices, and a transit gateway. Cisco SD-WAN Manager creates all the components when you pick the account and region to instantiate the cloud gateway. You can attach the appropriate device template to any free, available CSR universally unique identifiers (UUIDs) that are synced from PnP Smart Account.

You can override the global settings with custom settings to pick a different image, instance size, and subnet pool for a specific deployment. Only one cloud gateway instance per region is supported.



Note Ensure that you are subscribed to the image desired for the cloud gateway in the AWS marketplace. If you are not subscribed, then the cloud gateway creation fails.

AWS Branch Connect Overview

The edge devices connect to the host VPCs in the cloud over secure point-to-point tunnels. IPSec tunnels are set up between edge devices and the AWS Transit Gateway. These tunnels carry the branch VPNs traffic and BGP routing traffic. Using BGP, the devices and the transit gateway exchange the routing information and build routing tables.

A branch device can have any number of VPNs that require connectivity to the host VPCs. Each of these VPNs is represented as a VPN attachment to the transit gateway. As part of the VPN attachment, AWS customer gateway and VPN gateway cloud objects are created, which allow VPN connectivity from the branch device to the transit gateway. The transit gateway and the branch devices of a given site are in different BGP ASNs. The mapping information of VPNs to the tags (host VPCs) is derived from the global mapping. This mapping is realized in the cloud.

When you configure a new service VPN in a branch device template, an update event is generated, which triggers mapping based on the connectivity matrix. Similarly, when you remove a service VPN from the device template, another update event is generated, which triggers unmapping.

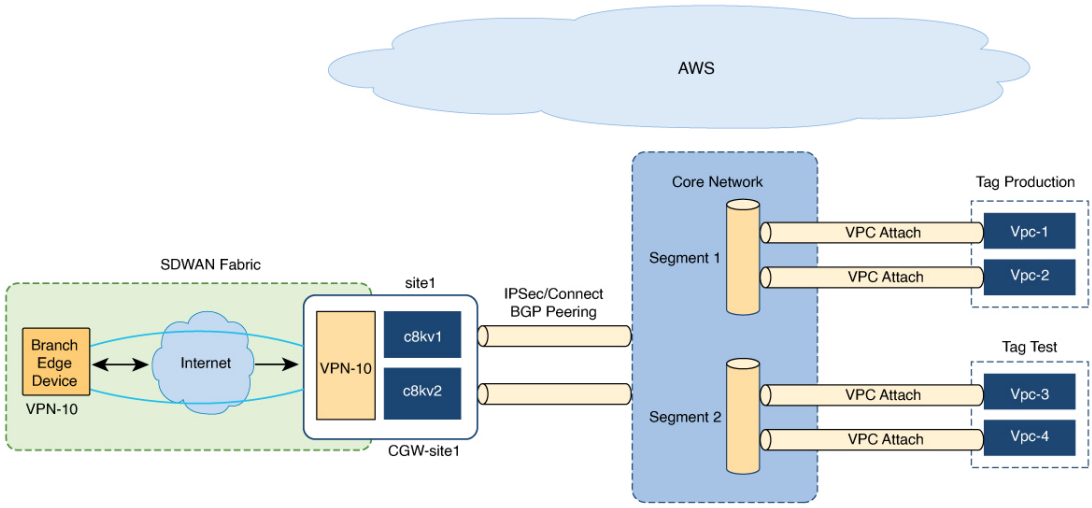


Note The number of branch edge WAN interfaces need to be proportional to the number of regions that the branch edge device needs to connect to. For example, if a branch needs to connect to hosts in two AWS regions, you need one WAN interface attached to each of the cloud gateway in that region. The WAN interfaces within a branch cannot have the same color.

AWS Cloud WAN

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

Figure 20: AWS Cloud WAN



AWS Cloud WAN is a managed WAN service that you can use to build, manage, and monitor a unified global network. You can easily connect and route traffic from different sites and regions over the AWS global network.

AWS Cloud WAN enables you to use simple network policies to configure and secure your network. The network policy is defined and populated in the backend, as you configure AWS integration using Cisco SD-WAN Manager workflows.

Using AWS integration workflows you can create global AWS Cloud WAN network, define different segments and attach different VPCs in different regions to these segments.

(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1) AWS Cloud WAN integration uses BGP-based dymanic routing to route traffic from different sites and regions instead of using static routes. In the AWS integration workflows, the cloud gateways have BGP peering with segments which allow IPSec based connectivity. This adds flexibility and redundancy to the workflows.

Upgrade Considerations from Cisco Catalyst SD-WAN Manager Release 20.12.1 to Cisco Catalyst SD-WAN Manager Release 20.13.1

- Disable the site-to-site communications (in global settings) for AWS in Cisco SD-WAN Manager before you upgrade to Cisco Catalyst SD-WAN Manager Release 20.13.1. After the upgrade is complete you can enable the site-to-site communications in global settings.

Information About Configuring Devices for AWS Integration Using Configuration Groups

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can use configuration groups in Cisco SD-WAN Manager to configure devices in AWS integration workflows. The use of same configuration groups between two cloud gateways is not supported.

You can enable configuration of devices using configuration groups in the global settings. When you create a cloud gateway, if you have enabled configuration using configuration groups in the global settings, you can choose an existing configuration group or create a new one. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups.

Note After you enable configuration of devices using configuration groups in the global settings, you can configure devices using both templates and configuration groups.

Software-Defined Cloud Interconnect Cloud Gateway Extension

From Cisco Catalyst SD-WAN Manager Release 20.15.1, in the Software-Defined Cloud Interconnect (SDCI) workflow, while creating a cloud gateway, you cannot configure devices using configuration groups.

Restrictions for AWS Integration

- The AWS Government cloud (AWS GovCloud) is not supported.

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, AWS GovCloud (US) is supported.

- AWS integration on IPv6 is not supported.
- Tags that are associated with host VPCs that have overlapping CIDRs cannot be mapped to each other.
- Overlapping IP addresses in different VPNs mapped to one host-VPC are not supported.
- AWS has a limit of 1000 routes per VPN connection. You need to provision a template with the aggregate-address or the network in BGP if you have more routes per VPN.
- AWS transit gateway has only 20 route tables by default.
- Auto-correct removal of cloud gateway through AWS console is not configured.
- Only one cloud gateway per region can be created.
- Only a single pair of Cisco cloud routers is instantiated.
- The CSR image version selected should be 16.12.02r or later.

- Cisco SD-WAN Manager configures one VPN tunnel per CSR 1000 device. This limits the bandwidth of the solution to 2.5 GBPS (1.25 GBPS throughput for each tunnel).
- Beginning with Cisco IOS XE Release 17.6.2, Cloud OnRamp for Multicloud supports integration with 10 AWS accounts.
- Multi cloud AWS Branch Connect Solution works only with Cisco SD-WAN branch or devices deployed using feature templates. The branches or devices based on configuration groups or CLI template are not supported.
- The CGW deployment with local zone enabled in AWS region is not supported.

Restrictions for AWS Cloud WAN

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

- You can only create cloud gateways from the same AWS account.
- The AWS Government cloud (AWS GovCloud) is not supported.
- AWS Cloud WAN supports only up to 20 segments per core network.
- The maximum number of supported peerings per core network is 50.
- You cannot create cloud gateways in regions that do not support AWS Cloud WAN. For information about currently supported regions, see the AWS documentation.
- The API support to get the status of the BGP sessions of the tunnels is not available in AWS. Therefore, the tunnel to AWS Cloud WAN network may be shown as reachable even when the cloud gateway is powered off in Cisco SD-WAN Manager.

Configure AWS Integration

AWS Configuration Prerequisites

You need the following to configure AWS integration using Cisco SD-WAN Manager.

- AWS cloud account details
- Subscription to AWS marketplace
- Cisco SD-WAN Manager must have two cloud router licenses that are free to use for creating a new account

Create AWS Cloud Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. The Cloud OnRamp for Multicloud dashboard displays.
2. Click **Associate Cloud Account** in the Setup pane. Note the external Id from the **Associate Cloud Account** page.

3. In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.
4. Enter the account name in the **Account Name** field.
5. (Optional) Enter the description in the **Description** field.
6. In **Use for Cloud Gateway**, choose **Yes** if you want to create cloud gateway in your account, or choose **No**.
7. Choose the authentication model you want to use in the field **Login in to AWS With**.
   - **Key**
   - **IAM Role**

   If you choose the **Key** model, then provide **API Key** and **Secret Key** in the respective fileds.

   Or

   If you choose the **IAM Role** model, then create an IAM role with Cisco SD-WAN Manager provided **External ID**. Note the displayed external Id from the window and provide the **Role ARN** value that is available when creating an IAM role.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, to create an IAM role, you must enter the External Idprovided by Cisco SD-WAN Manager into a policy by using the AWS Management Console.



Note When deploying Cloud OnRamp for Multicloud for an AWS account, if EC2 instance that hosts Cisco SD-WAN Manager is using Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) then the hop limit needs to be updated to 2 so that the IAM role credentials can be retrieved and used for communication with Cisco SD-WAN Manager. EC2 instances using Amazon EC2 Instance Metadata Service Version 1 (IMDSv1) do not require this step.

Do the following:

a. Attach an IAM Role to an existing Cisco SD-WAN Manager EC2 instance.
   1. See the Creating an IAM role (console) topic of AWS documentation to create a policy. In the AWS **Create policy** wizard, click **JSON** and enter the following JSON policy document.

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]
```

```
}
```

2. See the Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console blog of AWS Security Blog for information about creating an IAM role and attaching it to the Cisco SD-WAN Manager EC2 instance based on the policy created in Step 1.



Note On the **Attach permissions policy** window, choose the AWS managed policy that you created in Step 1.



Note The following set of permissions are allowed:

- AmazonEC2FullAccess
- IAMReadOnlyAccess
- AWSNetworkManagerFullAccess
- AWSResourceAccessManagerFullAccess

For more information on creating an AWS IAM Role, refer Creating an AWS IAM Role.

b. Create an IAM role on an AWS account that you want to use for the multicloud environment.

1. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 2.
2. See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

   In the **IAM Roles** window, scroll down and click the role you created in the previous step.

   In the **Summary** window, note the **Role ARN** that is displayed at the top.



Note You can enter this role ARN value when you choose the authentication model as IAM role in Step 7.

3. After modifying the trust relationship, click **JSON** and enter the following JSON document. Save the changes.



Note The account Id in the following JSON document belongs to the Cisco SD-WAN Manager EC2 instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
```

```
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
            "sts:ExternalId": "[vManage provided External ID]"
          }
        }
      }
    ]
}
```

8. Click **Add**.

To view or update cloud account details, click **...** on the Cloud Account Management page.

You can also remove the cloud account if there are no associated host VPC tags or cloud gateways.

Note During Multicloud resource cleanup process, Cisco SD-WAN Manager compares the current database to running resources in the account with org name and account detail tags. If there are any resources that matches the tags, but not in the current database are deleted. Therefore, the AWS Multicloud resources of Cisco SD-WAN Manager can be deleted by another Cisco SD-WAN Manager, if the organization name and the associated AWS account details are same. We recommend that if you are using the same AWS account across different Cisco SD-WAN Manager overlays, ensure that you use different organization and overlay name for each Cisco SD-WAN Manager.

Configure Cloud Global Settings

To configure cloud transit gateway global settings, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Cloud Global Settings** in the **Setup** pane. The **Cloud Global Settings** window appears.
2. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

   Enable the **Enable Configuration Group** option to use configuration groups to configure devices.
3. In the **Cloud Provider** field, choose **Amazon Web Services**.
4. Click **Cloud Gateway Solution** drop-down list to choose the AWS Transit Gateway and CSR in Transit VPC, or, beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, one of the following options.

   Beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, a combination of options is not supported. For example, if there are cloud gateways that were created using VPN connections, you must delete these cloud gateways before you can create AWS Transit Gateway Connect connections.

   - **Transit Gateway–VPN based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach.
   - **Transit Gateway–Connect based (using TVPC)**—Allows connectivity of the cloud gateway to the VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. The cloud

gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS TGW Connect (GRE tunnels) approach.

- **Transit Gateway–Branch-connect**—Allows connectivity of different Cisco Catalyst SD-WAN edge devices to VPCs in the cloud through the transit gateway that is instantiated in the AWS cloud. This option uses the AWS VPN connection (IPSec) approach.
- (Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1)

  Cloud WAN–VPN based (using TVPC)—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS VPN connection (IPSec) approach.
- (Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1)

  Cloud WAN–Connect based (using TVPC)—Allows connectivity of the cloud gateway to the VPCs in the cloud through AWS Cloud Wan. The cloud gateway consists of a pair of cloud services routers that are instantiated within a transit VPC. This option uses the AWS Connect attachments (supporting GRE tunnels) approach.

5. Beginning with Cisco vManage Release 20.8.1, the following fields are available:
   - Click the **Reference Account Name** drop-down list to choose the reference account name. Cisco SD-WAN Manager discovers the software images and instance sizes using this reference account name.



Note You can still choose a different account, if required, at the time of a cloud gateway creation.

   - Click the **Reference Region** drop-down list to choose the reference region. Cisco SD-WAN Manager discovers the software images and instance sizes in this reference region under the referenced account name.

6. In the **Software Image** field, do the following:
   a. Click **BYOL** to use a bring your own license software image or **PAYG** to use a pay as you go software image.
   b. From the drop-down list, select a software image.
7. Click the **Instance Size** drop-down list to choose the required size.
8. Enter the **IP Subnet Pool**.
9. Enter the **Cloud Gateway BGP ASN Offset**.
10. Choose the **Intra Tag Communication**. The options are **Enabled** or **Disabled**.
11. Choose the **Default Route**. The options are **Enabled** or **Disabled**.
12. Click **Update**.

Parameter	Description
Software Image	Specifies the preinstalled or the subscribed software images for your account.

Parameter	Description
Instance Size	

Parameter	Description
	Specifies the instance size. The options are: • t2.medium • t3.medium • c4.2xlarge • c4.4xlarge • c4.8xlarge • c4.xlarge • c5.2xlarge • c5.4xlarge • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge • c5n.9xlarge • c5n.large • c5n.xlarge **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, following instance types are supported: • t3.medium • c5.2xlarge • c5.4xlarge **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, c5.4xlarge is not supported. • c5.9xlarge • c5.large • c5.xlarge • c5n.2xlarge • c5n.4xlarge

Parameter	Description
	• c5n.9xlarge • c5n.large • c5n.xlarge Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, following instance is supported: • c5n.18xlarge **Note** Upgrade Cisco Catalyst SD-WAN Cloud devices running on Cisco SD-WAN Manager Release 19.2.1 on c3.2xlarge to Cisco SD-WAN Manager Release 20.4.1 or later in the following order. **1.** Resize c3.2xlarge to c5.4xlarge **2.** Upgrade the software to Cisco SD-WAN Manager Release 20.4.1 or later. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, following instance types are supported: • t3.medium • c5.large • c5.xlarge • c5.2xlarge • c5.9xlarge • c5n.4xlarge • c5n.18xlarge • c6in.large • c6in.xlarge • c6in.2xlarge • c6in.8xlarge
Cloud Gateway Solution	Specifies the combination of the Cloud Gateway Solution. For example, AWS Transit Gateway and CSR in Transit VPC.

Parameter	Description
IP Subnet Pool	Specifies the list of IP subnets separated by comma in CIDR format. More than one subnets can be specified. A single /24 subnet pool is able to support one cloud gateway only. You cannot modify the pool when a few cloud gateways are already making use of pool. Overlapping of subnets is not allowed.
Cloud Gateway BGP ASN Offset	Specifies the offset for allocation of transit gateway BGP ASNs. It is used to block routes learnt from one transit gateway (eBGP) to another. A band of 30 ASNs are reserved for transit gateway ASNs. Starting offset plus 30 will be the organization side BGP ASN. For example, if the offset is 64830, Org BGP ASN will be 64860. Acceptable start offset range is 64520 to 65500. It must be a multiple of 10.
Tunnel Count	This field appears if you choose **Transit Gateway–Connect based (using TVPC)** from the **Cloud Gateway Solution** drop-down list. Enter the number of tunnels for a VPN connection. You can configure up to 4 tunnels for each VPN connection. Each tunnel supports up to 5 Gbps of traffic. **Note** Changing the value of this parameter does not affect existing cloud gateways. To update the tunnel count for an existing cloud gateway, edit the cloud gateway from the **Configuration** > **Cloud OnRamp For Multicloud** > **Cloud Gateway** page.
Intra Tag Communication	Specifies if the communication between host VPCs under the same tag is enabled or disabled. If any tagged VPCs are already present and cloud gateways exist in those regions, then this flag cannot be changed.
Program Default Route in VPCs towards TGW	Specifies if the main route table of the host VPCs is programmed with default route is enabled or disabled.
Full Mesh of Transit VPCs	Specifies the full mesh connectivity between TVPCs of cloud gateways in different regions to carry site to site traffic (through CSRs).

Table 63: Expected Behavior for Global Settings

Item	Changeable after cloud gateway is created (Yes/No)	Default (Enabled/Disabled)
Software Image	Yes	NA
Instance Size	Yes	NA
IP Subnet Pool	See the description below	NA
Cloud Gateway BGP ASN Offset	No	NA
Intra Tag Communication	Cannot be changed if both cloud gateways and tagged host VPCs exist in any region	Enabled at the API level
Program Default Route in VPCs towards TGW	No	Enabled at the API level
Full Mesh of Transit VPCs	Yes	Disabled

Global IP Subnet Pool – can only be updated if there is no cloud gateway using global subnet pool. A cloud gateway uses global subnet pool whether it has custom setting or not. The subnet pool value is similar to the one in global setting (you can compare after splitting the list of CIDRs by comma; for example, *10.0.0.0/8, 10.255.255.254/8* and *10.255.255.254/8, 10.0.0.0/8* are similar).

If there is no cloud gateway using global subnet pool, the updated subnet pool in the global setting should not overlap with any of the existing custom subnet pools.

Custom IP Subnet Pool – when a custom setting is created, its subnet pool should not overlap with any of the existing custom subnet pools. It cannot partially overlap with the configured global subnet pool.

Discover Host Private Networks

You can discover host VPCs in all the accounts across all the respective regions of the account that are available. When the **Host VPC Discovery** is invoked, the discovery of the VPCs is performed without any cache.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Host Private Networks** under **Discover**. The **Discover Host Private Networks** window appears with the list of available VPCs.

   The host VPC table includes the following columns:

   - Cloud Region
   - Account Name
   - Host VPC Name
   - Host VPC Tag
   - Account ID
   - Host VPC ID

Click a column to sort the VPCs, as required.

2. Click the **Region** drop-down list to select the VPCs based on particular region.
3. Click **Tag Actions** to perform the following actions:
   - **Add Tag** - group the selected VPCs and tag them together.
   - **Edit Tag** - migrate the selected VPCs from one tag to another.
   - **Delete Tag** - remove the tag for the selected VPCs.

A number of host VPCs can be grouped under a tag. All VPCs under the same tag are considered as a singular unit. A tag ensures connectivity and is essential to view the VPCs in **Intent Management**.

Create Cloud Gateway

Cloud gateway is an instantiation of Transit VPC (TVPC), CSRs within TVPC and transit gateway in the cloud. To create a cloud gateway, perform the following steps.

Note Before beginning this procedure, ensure that you have two devices with templates attached, which have the same type of license (BYOL or PAYG).

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Create Cloud Gateway** under **Manage**. The **Manage Cloud Gateway - Create** window appears.
2. In the **Cloud Provider** field, choose Amazon Web Services from the drop-down list.
3. In the **Cloud Gateway Name** field, enter the cloud gateway name.
4. (Optional) In the **Description**, enter the description.
5. Choose the account name from the **Account Name** drop-down list.
6. Choose the region from the **Region** drop-down list.
7. (Optional) Choose the SSH Key from the drop-down list.
8. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
9. In the **Software Image** field, do the following:
   a. Choose a licensing option: **BYOL** for bring your own license or **PAYG** for pay as you go.
   b. In the drop-down menu, choose a software image.

Note The software image options are determined by the selection of **BYOL** or **PAYG**.

Note For information about onboarding a Cisco Catalyst 8000V without using Cisco Cloud OnRamp for Multicloud, see the Cisco SD-WAN Getting Started Guide.

10. Click the **Instance Size** drop-down list to choose the required size. Pick the size of the WAN edge based on the capacity needs.
11. Enter the **IP Subnet Pool**. Subnet pool is used for transit VPC creation, needs between /16 to /24.System allocates /27 per transit VPC 8 subnet(s).
12. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

    If you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for AWS, from the **Configuration Group** drop-down list, perform one of these actions:

    - Choose a configuration group.
    - To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow.

Note When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables configuration groups for all other multicloud and interconnect providers.

    a. Select the **Chassis number** to associate a pair of chassis to the configuration group.
    b. Click **Configure Device Parameters** and enter the following:
        1. **System IP**
        2. **Hostname**
        3. **TLOC Color**
        4. **Username**
        5. **User Password**
    c. Click **Create Gateway**.

13. The option is applicable only to configuration using device templates.

    Choose the UUID details in the **UUID (specify 2)** drop-down list.

Note

- Only logical devices (UUIDs) with a template attached appear in the list.
- From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

14. (Minimum release: Cisco vManage Release 20.10.1) In the **Multi-Region Fabric Settings** area, for **MRF Role**, choose **Border** or **Edge**.

    This option is available only when Multi-Region Fabric is enabled.

15. Click **Add** to create a new cloud gateway.

Note Creating cloud gateways for AWS Cloud WAN can take over an hour depending on the resources deployed. The first deployment in a region can fail if AWS verifying and validating the resources in this region.

You cannot create cloud gateways in regions that do not support AWS Cloud WAN. For information about currently supported regions, see the AWS documentation.

Configure Site Attachment

Perform the following steps to attach sites to a cloud gateway:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Gateway Management** under **Manage**. The **Cloud Gateways** window appears. A table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.

   For each of the cloud gateways, you can view, delete, or attach more sites.

2. For the desired cloud gateway, click **...** and choose **Cloud Gateway**.
3. Click **Attachment**.
4. Click **Attach Sites**.
5. In the **Circuit Color** drop-down list, choose a circuit color. A circuit color defines the search criteria for the sites you want to connect to your cloud gateway.
6. Click **Next**. The **Attach Sites - Select Sites** window appears. The table shows the sites with the selected circuit color.
7. Choose one or more sites from **Available Sites** and move them to **Selected Sites**.
8. Click **Next**.
9. On the **Attach Sites - Site Configuration** window, enter the **Tunnel Count**. The tunnel count ranges from 1 to 8 and each tunnel gives a bandwidth of 2.5 Gbps.
10. For the **Accelerated VPN** option, choose **Enabled** or **Disabled**. AWS Global Accelerator helps in optimized connectivity to the cloud.

11. Click **Next**. The **Attach Sites - Configuration Override** window appears. You can override the configuration that you performed in previous step, if required. You can alter the values for tunnel count and accelerated VPN status.
12. Click **Next**. The **Next Steps** window appears, where you can save the attachments you've added and exit the flow.
13. Click **Save and Exit**. If the configuration is successful, you see a message that indicates that the branch endpoints were successfully attached.



Note To view the tunnel status, go to the **Cloud OnRamp for Multicloud** Dashboard or the **Site Details** window.

Detach Sites

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. Click **Gateway Management** under **Manage**. The **Cloud Gateways** window appears. The table displays the list of cloud gateways with cloud account name, ID, cloud type, transit gateway.
2. For the desired cloud gateway, click **...** and choose **Cloud Gateway**. Next, click **Attachment**. The **Attachments - Cloud Gateway Name** window appears. The window displays the list of sites attached to the cloud gateway.
3. Click **Detach Sites**. The **Are you sure you want to detach sites from cloud gateway?** window appears.
4. Click **OK**. The sites attached to a cloud gateway are detached. The unmapping of the site happens and the VPN configuration is removed from the device.

Remove Cloud Gateway

On the **Cloud Gateways** window, for the desired cloud gateway, click **...**, and choose **Delete**. You must detach all the sites from a cloud gateway before trying to delete the cloud gateway.

You can view the cloud resources in the Cloud Resources Inventory for each cloud gateway in Cisco SD-WAN Manager.

Intent Management - Connectivity

Mapping workflow in Cisco SD-WAN Manager enables connectivity between Cisco Catalyst SD-WAN VPNs (segment) and VPCs, and VPCs to VPCs. VPCs are represented based on the tags.



Note Mapping of a new intent for a mapping task in progress is disabled. When intra-tag is enabled and when VPCs within the same region are added to the same tag, the mapping happens as part of tagging.

When the system records the intent for connectivity, mapping is realized in cloud in regions where cloud gateway is present. Mapping intents can be entered without cloud gateways being present in different regions. The user mapping intent is preserved and realized when a new cloud gateway or mapping change is discovered. As and when cloud gateways get instantiated in different regions, the mapping intents are realized in those

regions. Similarly, tagging operations can influence the mapping in different regions as well and mappings as per the tags are realized in the cloud.

In the Cloud OnRamp for Multicloud dashboard, click **Connectivity** under **Management**. The **Intent Management - Connectivity** window appears. The window displays the connectivity status with the following legends:

- Blank - Editable
- Grey color - System Defined
- Blue color - Intent Defined
- Green color - Intent Realized
- Red color - Intent Realized With Errors

On the **Connectivity** window, you can:

- View the changes in connectivity as required.
- Filter and sort.
- Define the connectivity independent of cloud gateways in different regions.
- Realize the connectivity in regions wherever cloud gateways are present.

Mapping is automatically realized when a cloud gateway exists in the same region or when tagging operations take place.

Connectivity information or the intent is entered in a matrix form with VPNs, tags as sources and tags as destinations. When you click on each cell, it provides a detailed information on - Mapped, Unmapped and Outstanding mapping.

VPCs involved in mapping (as part of tags) should have at least one subnet. VPCs with overlapping CIDRs lead to failed mapping.

Starting from Cisco IOS XE Catalyst SD-WANRelease 17.3.2, the mapping is region agnostic and can span a number of regions than confined to a given region. Instead of multiple mapping requests, a single mapping request involving a number of regions is dispatched towards the cloud agent. The information of all the VPCs, VPNs and connectivity elements across regions is put together in the same mapping request. The mapping status is enhanced to get the connectivity information and the current attachment specifications of the entire network of all the regions.

Depending on the mapping, more than one region can be locked at the same time. Inter-region mapping changes the mapping of local to regions to across regions as applicable. The regions are locked where a mapping is done across multiple regions. As audit is global in nature, all regions are locked while the audit is on.



Note AWS cloud operations can take up to 40-60 minutes to complete mapping the intent management.

Note Users are responsible for adding specific routes to transit gateway endpoint outside IPs for the tunnels to come up between the branched service and AWS transit gateway while using multiple WAN interfaces. Branch connect mapping only configures the required IPsec tunnel configuration to transit gateway endpoints.

Note The maximum number of supported peerings per core network is 50. If the number of VPN connections exceed this limit, the mapping fails.

Note During the mapping, the Multicloud workflow adds a default route in the VPC main route table. However, this does not happen if the main route table already has a default route. The VPC main route table should not have existing default route before mapping is applied.

IPsec Tunnels Down Due to Weaker Crytpo

When you upgrade Cisco SD-WAN Manager with multi cloud AWS VPN connect or branch connect to Cisco vManage Release 20.11.1 and the Cisco Catalyst 8000V Edge Software to Cisco IOS XE Catalyst SD-WAN Release 17.11.x from earlier 17.x releases, the IPsec tunnels between the TGW (transit gateway) of the Cisco Catalyst SD-WAN device and Cisco Catalyst SD-WAN devices in the cloud gateway will go down.

To bring up the tunnels, do either of the following:

- If you want to continue with older crypto configuration, use the **crypto engine compliance shield disable** command in the Cisco Catalyst SD-WAN devices of the cloud gateway and reload the devices to bring up the tunnels. The tunnels will come up with a weaker crypto. Any inconsistencies that appear in the cloud connections triggers an audit. When the audit triggers, all tunnels from group 2 will change to group 15 crypto and tunnels will still be down. To resolve this issue after the audit, unmap and map the connections using the Intent Management Cloud Connectivity page in Cisco SD-WAN Manager.
- When you upgrade Cisco SD-WAN Manager with multi cloud AWS VPN connect or branch connect to Cisco vManage Release 20.11.1 and the Cisco Catalyst 8000V Edge Software to 17.11 from earlier 17.x releases, instead of using the CLI command you can directly unmap and map the connections using the Intent Management Cloud Connectivity page in Cisco SD-WAN Manager. The tunnels will come up with group 15 crypto.

Note Use the above steps to bring up tunnels with the stronger crypto when you upgrade the AWS CGWExtn in SDCI. Software-Defined Cloud Interconnect (SDCI) has a solution called AWS CGWExtn that is deployed from SDCI. When you create a cloud gateway in Cisco SD-WAN Manager that uses SDCI, the tunnels will be down as AWS is deployed. You can access the gateways from the Intent Management Cloud Connectivity page in Cisco SD-WAN Manager.

Transit Gateway Peering

Table 64: Feature History

Feature Name	Release Information	Description
Transit Gateway Peering	Cisco IOS XE Release 17.3.2 Cisco vManage Release 20.3.2	This feature enables the ability to establish peer connections between transit gateways in different AWS regions. With this feature, you can connect to various Transit Virtual Private Clouds (TVPCs) and on-premise networks using a single gateway. The ability to peer transit gateways between different AWS regions enables you to extend the connectivity and build global networks spanning multiple other regions. To support inter-region connectivity, mapping and audit functions are enhanced.

Inter-region connectivity for multicloud networking allows communication among VPCs spread across a number of regions. It supports the following connectivity options:

- intra-tag communication within VPCs using a single tag across multiple regions.
- tag to tag connectivity with VPCs within them spread across a number of regions.

The VPC and VPN attachments are associated with and propagated to different routing tables within the transit gateway. Depending on the desired connectivity, there are routes within transit gateway route tables towards the VPC and TVPC classless inter-domain routes (CIDRs) of other regions pointing to respective transit gateway peered attachments. This allows VPCs and cloud service routers in one TVPC region to communicate with VPCs and cloud service routers in other TVPCs in other regions. TVPCs are connected in a mesh, whereas connectivity of host VPCs follows the connectivity or the intent matrix defined.

The VPN-to-tag connectivity is limited to VPN-to-VPCs connectivity (VPCs within the tag) within that region. The VPN connectivity does not traverse the transit gateway peered attachments.

The audit functionality is configured at a global level and is enhanced to reinstate the broken transit gateway peered attachments, ensuring inter-CSRs connectivity. For more details on Audit, see Audit Management.

Audit Management

In the Cloud OnRamp for Multicloud dashboard, the audit screen helps to bring the cloud state in sync with the Cisco SD-WAN Manager state. When the mapping fails because of a tagging mismatch or missing host VPCs, audit helps in fixing the mapping for recoverable errors and mismatched tagging issues.

In the **Cloud OnRamp for Multicloud** window, for the desired cloud type, click **...** and choose **Audit**. The Audit report for the desired cloud type appears.

Audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what has been realized in the cloud. The gaps are in terms of cloud resources, their mappings, or connectivity and states. When such gaps are detected, Cisco SD-WAN Manager flags such gaps and takes recovery actions to bring the cloud state in sync with the intents configured. For example, if there's an intent to map all host VPCs in some account or region tagged with some tag to get mapped to some given transit gateway and a new host

VPC tagged with the same tag is found disconnected with transit gateway, Cisco SD-WAN Manager connects the new host VPC back with the transit gateway.

Types of Audit:

- On-Demand
  - Invoked by the user.
  - If the report is out of sync, you can initiate audit-with-fix-option to fix the issue.
- Periodic - Invoked by the system automatically, periodically every 2 hrs. The first periodic audit will start in 15 minutes after the system startup.

The audit functionality is configured at a global level and is enhanced to reinstate the broken transit gateway peered attachments, ensuring inter-CSRs connectivity.

(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1) For AWS Cloud WAN, you can view and compare the policy documents on Cisco SD-WAN Manager and the core network policy that are available on cloud resources inventory for each cloud gateway. You can identify the discrepencies in these policy documents and troubleshoot accordingly.

For more information on AWS integration, see:

- Amazon Virtual Private Cloud Getting Started Guide
- Amazon Virtual Private Cloud Network Administrator Guide
- Transit gateway VPN Attachment

Multicloud Audit-reported Anomalies and Fixes

Table 65: Examples of AWS audit discrepancies

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Transit Gateway Attachment with Resource Type as **VPC** in AWS (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details**: Mapping issue Connectivity element was missing from response: [srcType:VPC ID dstType: <C8kv-device1-UUID]> Connectivity element was missing from response: [srcType: <C8kv-device1-UUID >dstType: VPCID]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the applicable solution type.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing site-to-site VPN Attachment (Transit Gateway Attachment Type VPN) in AWS	Transit Gateway–VPN based (using TVPC) / Cloud WAN–VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: Mapping **Details**: Mapping issue vpnAttachSpec with tunnelId: <C8kv-device1-UUID >:<VPNID> was missing from the cloud.	Yes, audit-fix workflow - 1 is triggered.
Missing Transit Gateway Attachment > VPC Attachment in secondary AWS account (Applicable when CGW and workload hosts are in different accounts) (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:VPC src: VPC1-Account1 dstType: VPC2 dst: VPC2] Connectivity element was missing from response: [srcType:VPC src: vpc-1 dstType: <C8kv-device1-UUID>]	Yes, audit-fix workflow - 1 or audit-fix workflow - 2 is triggered depending on the solution type.
Missing Transit Gateway Attachment with resource type as **Connect** in AWS	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC)	**Report Type**: Mapping **Details:** Mapping issue Connectivity element was missing from response: [srcType:<C8kv-device1-UUID> dstType:VPC dst:VPCID] Connectivity element was missing from response: [srcType: C8kv-device2-UUID> dstType:VPC dst:VPCID]	Yes, audit-fix workflow - 2 is triggered.

Anomaly / Trigger	Applicable Solution Type	Audit Findings / Error Message	Fixability (Fix, when applicable, is common for both on-demand and periodic scenarios)
Missing Host VPC (Not applicable to enhancements to enable connectivity to an existing AWS Transit Gateway which is supported from Cisco Catalyst SD-WAN Manager Release 20.18.1.)	All	**Report Type**: HOSTVPC **Details:** Host Vpc issue: <VPC ID> Hostvpc: <VPC ID> Tag mismatch- [<TAG NAME>! =] Hostvpc: <VPC ID> Couldn't find in the cloud.	Yes, audit will remove the missing VPC from tag(s) and from discovered VPC list.
Missing TGW	Transit Gateway–VPN based (using TVPC) / Cloud WAN VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TGW **Details:** Cloud Gateway (TGW) issue: TGW missing from the cloud. Name: <TGW Name>, region: <Region>. Please recreate the Cloud Gateway	Not fixable
Missing C8kv	Cloud WAN–Connect based (using TVPC) / Transit Gateway–Connect based (using TVPC) / Transit Gateway–VPN based (using TVPC) / Cloud WAN – VPN based (using TVPC) / Transit Gateway Branch-Connect	**Report Type**: TVPC **Details:** Cloud Gateway (TVPC) issue. Name: <CGW Name>, Id:<TVPC Id>. Please recreate the Cloud Gateway.	Not fixable
Invalid credentials	All	Could not perform audit at this time. Please retry after 10 minutes. Audit Failure.	Not fixable

Note Network connectivity disturbance is expected when the audit-fix (on-demand or periodic) is in progress, as the fix workflow deletes and recreates attachments and mappings in all the regions.

Note VPCs referred to are those discovered and tagged by Cisco SD-WAN Manager. “Missing” is defined in the context of the Cisco SD-WAN Manager’s database/knowledge.

Note Audit-fix performs the same steps in both on-demand (that is, clicking the **Fix Sync Issues** button) and periodic audit scenarios.

Note Audit-fix deletes all out-of-band attachments (VPC, TGW-peering, and Connect) to TGW or CloudWAN that users have manually created or mapped outside of CoR workflow, if any exist.

Monitor AWS Integration using Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

Multicloud Deployments

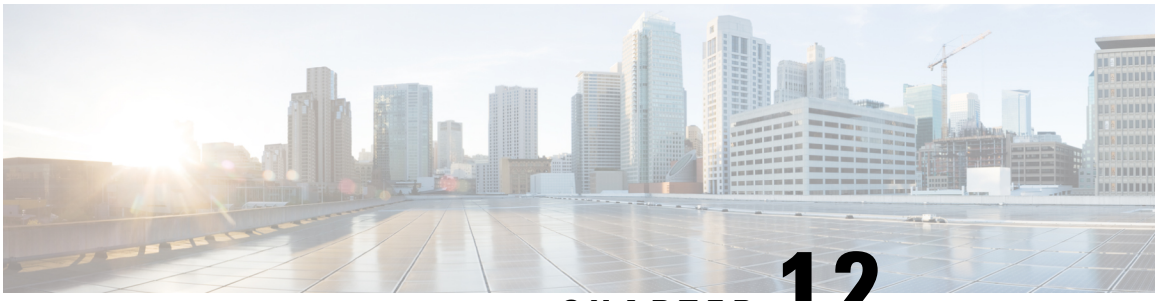
You can view the following information about multicloud deployments from **Monitor** > **Multicloud** on Cisco SD-WAN Manager:

- For each cloud type:
  - Number of cloud gateways and the health of each gateway.
  - Number of WAN edge devices and its health.
  - Number of sites connected to cloud gateways.
  - Number of VPN connection tunnels through cloud gateways.
  - Number of connected tags.
  - Number of mapped host VPCs or vNETs.
  - Number of VPN connections.
- For AWS Cloud WAN solution, you can view the operational AWS Cloud WAN core network policy in the AWS cloud.

Multicloud Dashboard

You can view the multicloud dashboard from **Configuration** > **Cloud OnRamp for Multicloud** on Cisco SD-WAN Manager. The multicloud dashboard summarizes the whole network snapshot where you can view information about each cloud gateway.

You can view the state of BGP sessions from each of the WAN edge devices for site-to-site communication through AWS Cloud WAN in **Additional Details** section on the dashboard.



CHAPTER 12

Amazon GovCloud (US) Integration

Table 66: Feature History

Feature Name	Release Information	Description
Support for AWS GovCloud (US) with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With the integration of Amazon Web Services (AWS) GovCloud (US) with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, you can store your highly sensitive workloads in an isolated cloud that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements of the U.S. government and its customers. The same features that are available with the AWS integration with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud are also available with Amazon GovCloud (US). Use the AWS Transit Gateway to connect your branch devices to the AWS GovCloud (US).

- Information About AWS GovCloud (US) Integration, on page 338
- Supported Devices for AWS GovCloud (US), on page 339
- Prerequisites for AWS GovCloud (US) Integration, on page 339
- Restrictions for AWS GovCloud (US) Integration, on page 340
- Use Case for AWS GovCloud (US) Integration, on page 340
- Configure AWS GovCloud (US), on page 340

Information About AWS GovCloud (US) Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud extends support for AWS GovCloud (US), allowing you to store and manage your highly sensitive workloads in AWS GovCloud (US).

The following are examples of highly sensitive workloads that you can store in AWS GovCloud (US):

- Controller Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export data

The same features and workflow that are available for the AWS integration are also available with the AWS GovCloud (US) integration with the exception of support for the Transit Gateway Network Manager (TGNM).

Note The TGNM is supported for AWS, but the TGNM is not supported for AWS GovCloud (US).

A transit gateway is a network transit hub that you can use to interconnect your Virtual Private Cloud (VPC) and on-premises networks. You can attach a VPC or a VPN connection to a transit gateway. The transit gateway acts as a virtual router for traffic flowing between your VPC and VPN connections. The transit gateway provides a way to interconnect VPCs and VPNs.

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud uses the AWS Transit Gateway to connect your branch devices to the AWS GovCloud (US). A configuration wizard in Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud automates the bring-up of the transit gateway to your AWS GovCloud (US) account and automates the connections between AWS GovCloud (US) applications and branch users in the overlay network.

For more information on the AWS GovCloud, see the AWS GovCloud (US) documentation.

Configure Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud with AWS GovCloud (US) using Cisco SD-WAN Manager.

Benefits of AWS GovCloud (US) Integration

- Allows you to move and store sensitive data workloads in AWS GovCloud (US) that meet the FedRAMP requirements of the U.S. government and its customers
- Supports the same features and workflow as for the AWS integration
- Supports advanced routing and path selection using a secure Cisco Catalyst SD-WAN tunnel from a data center to the cloud

- Supports telemetry data exchange between a data center and AWS GovCloud (US)

Supported Devices for AWS GovCloud (US)

Supported Platforms

For more information on the supported platforms for AWS GovCloud (US), see Overview of AWS Integration.

Supported Instances for AWS GovCloud (US)

- c5.large
- c5.xlarge
- c5.2xlarge
- c5.9xlarge
- c5n.large
- c5n.xlarge
- c5n.2xlarge
- c5n.4xlarge
- c5n.9xlarge
- c5n.18xlarge
- t3.medium



Note AWS and AWS GovCloud (US) instance sizes are the same.

Prerequisites for AWS GovCloud (US) Integration

- You must have an AWS GovCloud (US) cloud account.



Note An AWS GovCloud (US) account is different from an AWS account.

- You must have a subscription to the AWS GovCloud (US) marketplace.
- You must have two Cisco SD-WAN Manager cloud router licenses that are free to use for creating a new account.

Restrictions for AWS GovCloud (US) Integration

- No support for the TGNM for AWS GovCloud (US).

Use Case for AWS GovCloud (US) Integration

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud with AWS GovCloud (US) allows you to move and store your compliance workloads in an isolated cloud that meets the FedRAMP requirements of the U.S. government and its customers.

The following are examples of sensitive data that you can store in AWS GovCloud (US):

- Controller Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export data

Configure AWS GovCloud (US)

The workflow for configuring AWS GovCloud (US) is the same as the workflow for configuring Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud with AWS.

1. Create an AWS GovCloud (US) cloud account.

   For more information on creating an AWS GovCloud (US) account, see Create AWS Cloud Account.

2. Configure global settings for the cloud transit gateway.

   For more information on configuring global settings for the cloud transit gateway, see Configure Cloud Global Settings.

3. Discover host Virtual Private Clouds (VPCs) in all the accounts across the AWS GovCloud (US) regions.

   For more information on discovering host VPNs in AWS, see Discover Host Private Networks.

4. Create a cloud gateway.

   For more information on creating a cloud gateway, see Create Cloud Gateway.

5. Attach sites to a cloud gateway.

   For more information on attaching sites to a cloud gateway, see Configure Site Attachment.

6. Enable connectivity between Cisco Catalyst SD-WAN VPNs and VPCs.

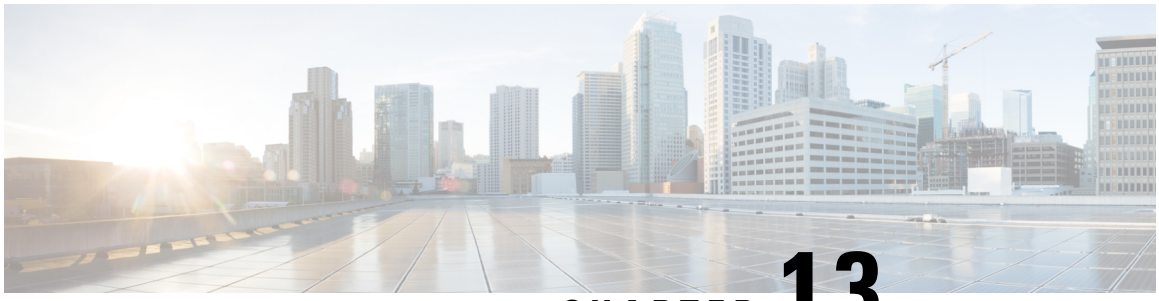
   For more information on enabling connectivity between Cisco Catalyst SD-WAN VPNs and VPCs, see Intent Management - Connectivity.

7. Enable peer connections between the transit gateways in different AWS GovCloud (US) regions.

   For more information on enabling peer connections between transit gateways in different AWS GovCloud (US) regions, see Transit Gateway Peering.

8. Conduct an audit to identify gaps or disconnects between the Cisco SD-WAN Manager intent and what has been realized in the cloud.

   For more information on conducting an audit management review, see Audit Management.



CHAPTER 13

Microsoft Azure Virtual WAN Integration

Table 67: Feature History

Feature Name	Release Information	Description
Automated Integration of Azure Virtual WAN and Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature enhances Cloud OnRamp integration with Microsoft Azure by allowing Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) to be deployed inside the Azure Virtual WAN Hub instead of deploying it in transit VNets. It also automates the Cisco Catalyst SD-WAN fabric connection to Azure Virtual WAN Hub through Cisco Catalyst 8000V. The connectivity between inter-region Azure Virtual WAN Hubs is also supported. In addition, you can convert the Azure virtual WAN hubs created using Cisco SD-WAN Manager into secured hubs by deploying Azure firewall inside them. However, secured virtual hubs can only be configured using the Microsoft Azure portal.
Integration of Cisco Catalyst SD-WAN and Azure Virtual WAN Hub Using Azure Portal	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	As part of the integration of Cisco Catalyst SD-WAN with Azure Virtual WAN, you can also use the Azure portal to upload bootstrap configuration files for Cisco Catalyst 8000V instances. These instances can then be used to create a virtual WAN hub using the Azure portal.
Routing Traffic Flow to a Virtual Hub Firewall or a Local Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to route Microsoft Azure Virtual WAN hub traffic to a firewall on a local branch router, or direct local branch traffic to an Azure secured virtual hub, to be subject to the security policies of the Azure Firewall Manager.
Azure Scaling, Audit, and Security of Network Virtual Appliances	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to edit the SKU scale value, and have better security for your Network Virtual Appliances (NVAs). The audit service compares the information from the Cisco SD-WAN Manager and Azure cloud databases and identifies the discrepancies.

Feature Name	Release Information	Description
Periodic Audit, Enhancement to Azure Scaling and Audit, and ExpressRoute Connection.	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	Cisco SD-WAN Manager provides an optional periodic audit every two hours. This automatic audit takes place in the background and generates a report of the discrepancies. If you enable the auto correct option, Cisco SD-WAN Manager automatically resolves any recoverable issues found during the periodic audit. You can fix the individual discrepancies generated after initiating an on-demand audit. Cisco SD-WAN Manager supports ExpressRoute connections from branch offices to NVAs through Cisco Catalyst SD-WAN tunnels. ExpressRoute connections are the private networks that offer higher reliability, fewer latencies, and faster connections for data transfer.
Support for Multiple Virtual Hubs in Each Region	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	You can create multiple virtual hubs in a single Azure region.
Added an Azure Instance Type	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	With this feature, new instance types are added which includes 16 CPU cores and 64 GB of memory. You can deploy this type of instance for SKU scale values of 20, 40, 60, and 80.
Configure Device for Azure Integration Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for Azure integration.

- Information About Azure Virtual WAN Integration, on page 345
- Supported Devices for Azure Virtual WAN Integration, on page 353
- Prerequisites for Azure Virtual WAN Integration, on page 354
- Restrictions for Azure Virtual WAN Integration, on page 355
- Use Cases for Azure Virtual WAN Integration, on page 356
- Configure Azure Virtual WAN Integration, on page 357
- Verify Azure Virtual WAN Integration, on page 372
- Monitor Azure Virtual WAN Integration Using Cisco SD-WAN Manager, on page 373

Information About Azure Virtual WAN Integration

Azure Virtual WAN Hub Integration with Cisco Catalyst SD-WAN

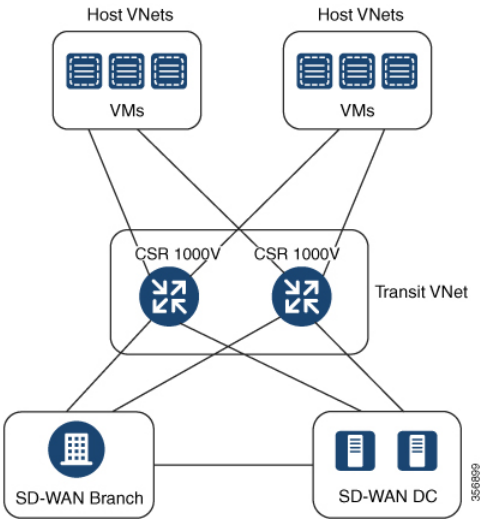
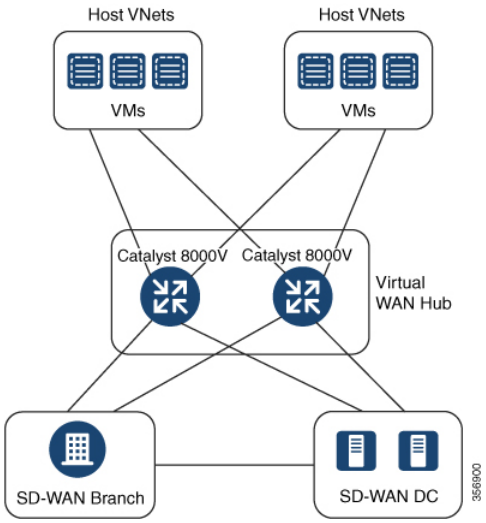
Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

The integration of the Cisco Catalyst SD-WAN solution with Azure virtual WAN enhances Cloud OnRamp for Multicloud deployments and enables configuring Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) as a network virtual appliance (NVA) in Azure Virtual WAN Hubs.

This integration simplifies the consumption model for cloud services because it eliminates the need to create a transit virtual network (VNet) and you can control your host VNet connectivity directly through the Azure Virtual WAN Hub. Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch connectivity through Microsoft Azure. It enables you to connect and configure branch devices that can communicate with Azure. Configuring Cisco Catalyst 8000V instances inside Azure virtual hubs provides higher speeds and bandwidth and overcomes the speed and bandwidth limitation of using transit VNets.

Cloud OnRamp for IaaS Versus Cloud OnRamp for Multicloud

This table lists the differences between Cloud OnRamp for IaaS and Cloud OnRamp for Multicloud in the context of Microsoft Azure Integration.

Cloud OnRamp for IaaS for Azure	Cloud OnRamp for Multicloud for Azure
	
Enables automated provisioning of transit VNets through the Cloud OnRamp for IaaS workflow in Cisco SD-WAN Manager	Enables automated provisioning of Azure virtual hubs through the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager
Cisco SD-WAN Manager automatically provisions two Cisco Cloud Services Router 1000V Series (Cisco CSR1000V) devices inside the transit VNet	Cisco SD-WAN Manager automatically provisions two Cisco Catalyst 8000V instances inside the Azure virtual hub

For information on Cloud OnRamp for IaaS with Azure and how to configure transit VNets, see Configure Cloud OnRamp for IaaS for Azure.

How Virtual WAN Hub Integration Works

The connection between the overlay network and a public-cloud application is provided by a pair of redundant Cisco Catalyst 8000V instances that are configured inside the Azure virtual WAN hub as part of the Cloud OnRamp for Multicloud workflow for Azure. Using redundant routers to form the transit offers path resiliency to the public cloud.

The Cloud OnRamp for Multicloud flow in Cisco SD-WAN Manager discovers your existing VNets in geographical cloud regions and allows you to connect select VNets to the overlay network. In such a scenario, Cloud OnRamp for Multicloud allows simple integration between legacy public-cloud connections and the Cisco Catalyst SD-WAN overlay network.

A configuration wizard in Cisco SD-WAN Manager automates the bring-up of the Azure Virtual WAN Hub to connect with your public cloud account. The wizard also automates the connections between public-cloud applications and the users of those applications at branches in the overlay network. Using tags, Cisco SD-WAN Manager enables you to map the service VPNs in your branches with specific VNets in your public cloud infrastructure.

VNet to VPN Mapping

The Intent Management workflow in Cisco SD-WAN Manager enables connectivity between Cisco SD-WAN VPNs (branch networks) and VNets, and VNets to VNets. VNets are represented by tags created under the Discover workflow for Cloud OnRamp for Multicloud. When VNets are mapped to connect them to the virtual WAN hubs, they are assigned a default route and propagate to the default label. When you create VNet tags within an Azure region, mapping is automatically created based on the other VNets and VPNs that share the same tag.

When Cisco SD-WAN Manager records the intent for connectivity, mapping is realized in cloud in regions where the cloud gateway is present. Mapping intents can be entered without cloud gateways being present in different regions. Your mapping intent is preserved and realized when a new cloud gateway or mapping change is discovered. As and when cloud gateways get instantiated or discovered in different regions, the mapping intents are realized in those regions. Similarly, tagging operations can influence the mapping in different regions as well and mappings as per the tags are realized in the cloud.



Note The VPNs selected to be mapped to VNet tags must not have overlapping IP addresses. This is because segmentation is not supported in Microsoft Azure Virtual WAN.

Inter-region Azure Hub-to-Hub connectivity is enabled by creating VNet tags and mapping them to your VPN sites. No additional configuration is required to enable inter-region hub-to-hub connectivity. VNets are associated with the Virtual WAN Hub for their respective regions. If VNets in different Azure regions share the same VNet tag, the connectivity between such VNets is automatically established and is carried out through the respective Virtual WAN Hubs that the VNets are connected to.

Components of Azure Virtual WAN Integration Workflow

A cloud gateway to connect your branches and data centers to the public cloud infrastructure is a logical object that hosts Cisco Catalyst 8000V instances. It comprises Azure Resource Groups, Azure Virtual WAN, and Azure Virtual WAN Hub.

Resource Groups

All Azure networking resources belong to a resource group and resource groups are created under Azure subscriptions. For Azure cloud gateways, Azure virtual WAN, and Azure Virtual WAN Hub are created under a resource group.

The first step to create an Azure cloud gateways is therefore to create a resource group.

After a resource group is created, you can configure Azure Virtual WAN.

Azure Virtual WAN

Azure Virtual WAN is the backbone of the Azure networking service. It's created under an existing Azure resource group. An Azure Virtual WAN can contain multiple Azure virtual hubs within it, as long as each virtual hub belongs to a different Azure region. Only one virtual hub per Azure region is supported.

After a virtual WAN has been defined under a resource group in a region, the next step is to create an Azure Virtual WAN Hub.

Azure Virtual WAN Hubs

The Azure virtual WAN Hub manages the core connectivity between your VPN sites and NVAs, and VNets. Once a virtual hub is created, the Cisco Catalyst 8000V instances can be integrated into the Azure networking service.

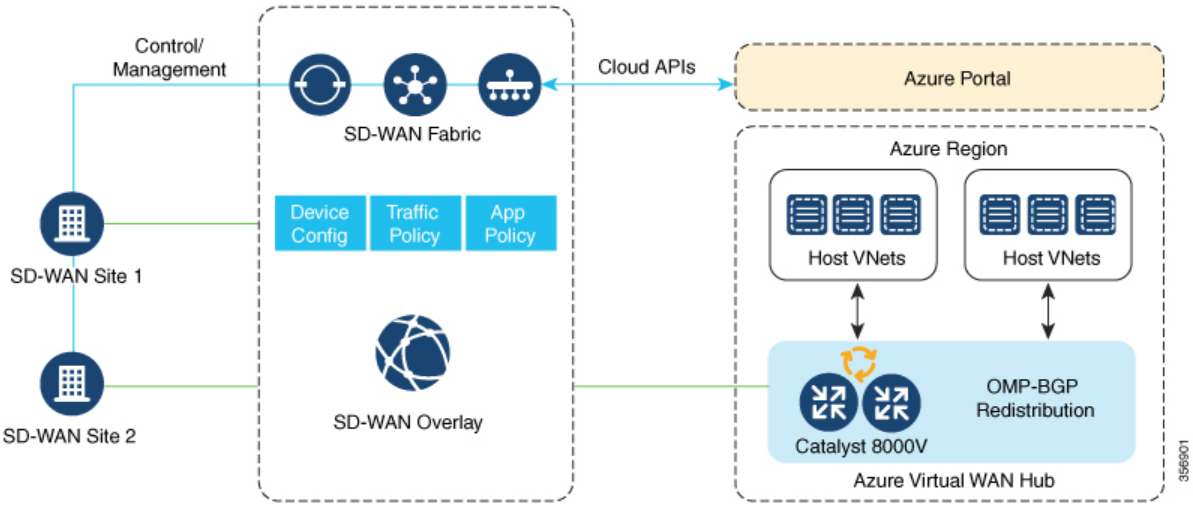
Connectivity Models

With the Integration of Azure Virtual WAN with the Cisco Catalyst SD-WAN solution, the following connectivity models are supported:

- Cisco Catalyst SD-WAN branch to Azure Host VNets within the same Azure region
- Inter-region Azure virtual hub-to-virtual hub connectivity

Cisco Catalyst SD-WAN Branch to Azure Host VNets (Single-region)

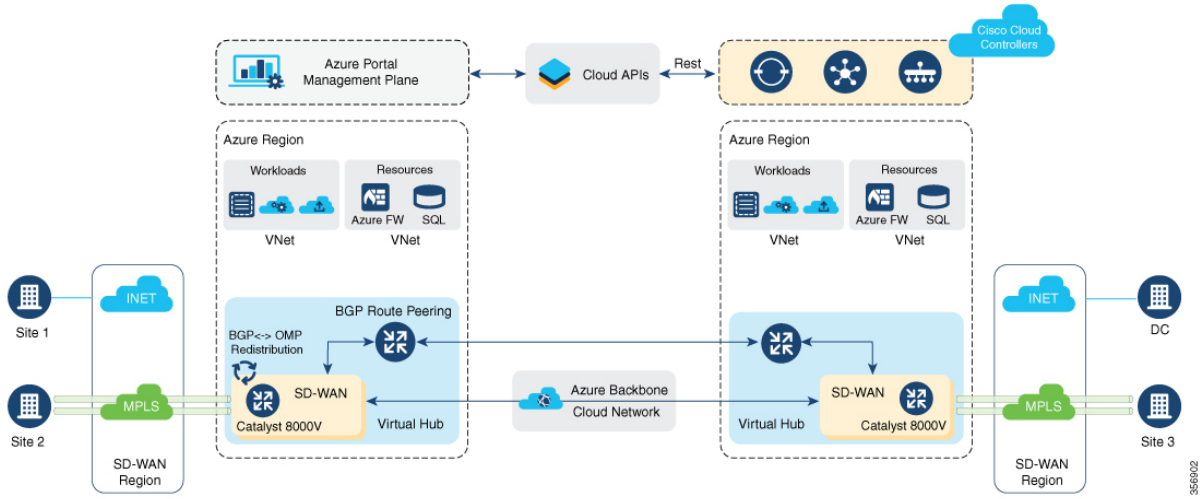
Figure 21: VNet to VNet Mapping within the Same Azure Region



In this scenario, the virtual hub is standalone and isn't connected to the virtual hubs in other Azure regions. In such cases, the VNets belong to the same region as the virtual hub, and are connected to your branch VPNs using VNet tags that are defined in Cisco SD-WAN Manager.

Virtual WAN Hub to Virtual WAN Hub (Inter-region)

Figure 22: Inter-region VNet-VNet Mapping Through Virtual Hubs



This image represents hub-to-hub connectivity with Azure backbone. This connectivity need not be configured separately. It's automatically achieved if VNets in different Azure regions share the same VNet tag.

Routing Traffic Flow to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

The Microsoft Azure environment includes a virtual hub that enables connectivity between Azure Virtual Network (VNet) workloads and local branch devices. The integration of Cisco Catalyst SD-WAN and the Azure environment enables the following firewall options:

- Routing outgoing internet traffic in the Azure Virtual WAN hub to a firewall on a local branch router
- Routing outgoing internet traffic from a local branch router to an Azure secured virtual hub, to be subject to the security policies of the Azure Firewall Manager.

Note An Azure secured virtual hub is an Azure Virtual WAN hub that has security and routing policy managed by the Azure Firewall Manager.

In both cases, return traffic follows the same path as outgoing internet traffic, so the same firewall policy applies to traffic in both directions.

Azure Virtual WAN Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

The multicloud audit service compares the information from the Cisco SD-WAN Manager database with the information in the Azure cloud database. This information includes Azure virtual WAN, virtual hubs, network virtual appliances, virtual networks, and VPN-to-virtual network mapping. Later, Cloud OnRamp for Multicloud compares the results, identifies the discrepancies, and displays a list of Microsoft Azure objects with and without errors.

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, the audit function incorporates the following enhancements:

- After you initiate an on-demand audit, the Cloud OnRamp for Multicloud audit service identifies and lists discrepancies between the information in the Cisco SD-WAN Manager database and the information in the Azure cloud. You can choose to fix all the discrepancies together or select a discrepancy and fix it individually. When you check a check box adjacent to an individual discrepancy, a brief explanation of the issue appears below the discrepancy.

  For more details about the audit discrepancies and resolutions, see Audit Discrepancies and Resolutions.

- You can now enable or disable periodic audits. For details, see Enable Periodic Audit.

Information About Periodic Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, Cisco SD-WAN Manager provides an optional periodic audit with an interval of two hours. This automatic audit takes place in the background and generates a report of the discrepancies. If you enable the auto correct option, Cisco SD-WAN Manager automatically resolves recoverable issues, if any, that are found during the periodic audit. For more details about the periodic audit and its resolutions, see Audit Discrepancies and Resolutions.



Note If you are upgrading the Cisco SD-WAN Manager version, the periodic audit and auto correct options are disabled by default. You can enable them from the **Cloud Global Settings** window. For details, see Add and Manage Global Cloud Settings.

Audit Discrepancies and Resolutions

The following table provides details about the audit discrepancies and resolutions for Azure.

Table 68: Examples of Azure audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
If the VNet is tagged in the Cisco SD-WAN Manager database, but it is not available in the Azure portal.	**Report Type**: VNet and Mapping **Details**: **VNet issue**: Cloud Virtual Network Issue: Not Found on Azure portal Name: <vnet-name>. Error received from Azure: Azure Error: ResourceNotFound Message: The resource '<vnet-name>' under resource group '<rg-name>' was not found. For more details, see https://aka.ms/ARMResourceNotFoundFix **Mapping issue**: Virtual Hub is mapped with virtual network <vnet-name> that does not exist.	The audit will remove the mapping from Cisco SD-WAN Manager. The audit will remove VNet from Cisco SD-WAN Manager.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
If the VNet tag is removed from the Azure portal, or if a VNet tag mismatch exists between Cisco SD-WAN Manager and Azure portal.	**Report Type**: VNet **Details**: Cloud Virtual Network Issue: Tag On Cisco SD-WAN Manager is not the same as Azure portal Name: <vnet-name>.	Virtual network <vnet-name> will be tagged with <tag-name>.	Virtual network <vnet-name> will be tagged with <tag-name>.
If the storage account is not available in the Azure portal but it is available in the Cisco SD-WAN Manager database.	**Report Type**: Storage **Details**: Cloud Gateway (Storage) issue: Not Found on Azure Portal.Name: <name>, Id: <id>. A storage account is required to configure bootstrap for NVA create or edit operations. Error received from Azure: Azure Error: ResourceNotFound Message: The resource '<storage-account-name>' under resource group '<rg-name>' was not found. For more details please go to https://aka.ms/ARMResourceNotFoundFix	Storage account <storage-account-name> will be removed from Cisco SD-WAN Manager.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.

Anomaly / Trigger	Audit Findings / Error Message	Resolution	
		On-Demand Audit Fix	Periodic Audit and Auto Correct
If virtual WAN, vHub, or NVA is not available in the Azure portal.	**Report Type**: VWAN, vHub, NVA, Mapping	Audit removes virtual WAN, vHub, NVA, mapping from the Cisco SD-WAN Manager database. **Note**: Do not delete the cloud gateway manually. Deleting the cloud gateway results in a discrepancy between the cloud providers and can impact the ability to provision anything further or impact other CoR operations.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You can use on-demand audit to fix the discrepancy.
Mapping is found in the Cisco SD-WAN Manager database but it is not found in the Azure portal.	**Report Type**: Mapping **Details**: Mapping issue: Cloud Virtual Networks to Virtual Hub mapping issue. Mapping not found on Azure Portal with vNet <vnet-name>	Run audit-fix-sync issues to add virtual hub mapping to the Azure portal.	Audit adds virtual hub mapping to the Azure portal.
Mapping is found in the Azure portal, but it is not found in theCisco SD-WAN Manager database.	Audit shows in sync	Audit reports are in sync. To add the mapping back to the Cisco SD-WAN Manager database, add tag manually and map VNet using the Cisco SD-WAN Manager workflow.	Periodic audit reports are in sync. To add the mapping back to the Cisco SD-WAN Manager database, add tag manually and map VNet using the Cisco SD-WAN Manager workflow.
Account credentials expired	**Report Type**: VWAN, vHub, NVA, Mapping	You are required to manually update the account credentials.	Periodic audit reports are out of sync, but auto correct will not fix the discrepancy. You are required to manually update the account credentials.

Note Audit support for Azure was introduced in Cisco vManage Release 20.7.1.

Note Audit is not applicable for SD-Routing CoR (vHub with VPN) only deployment.

SKU Scale Value of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

You can edit the SKU scale value of a Cisco Catalyst 8000V Edge instance in Azure. In releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1, the SKU scale value is not editable. If you want to change the SKU scale value, you must delete and re-create the cloud gateway with a new SKU scale value.

You can opt for higher SKU scale values for better performance and lower values for cost-effectiveness.

For more information on how to update SKU scale values, see Configure SKU Scale Value.

Note After editing the SKU scale value, expect a network downtime of 3 to 4 minutes.

For details about the supported SKU scales, see Supported Azure Instances for Azure Virtual WAN Integration.

Security Rules Configuration of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Microsoft Azure has an option to edit the security rules of Network Virtual Appliances (NVAs). Cisco SD-WAN Manager supports the configuration of these security rules for NVAs.

Cisco Catalyst 8000V NVAs that are launched during cloud gateway creation prohibit the use of all the inbound ports, except Cisco Catalyst SD-WAN-related ports. The Security Rules Configuration of NVA feature allows you to enable a particular port as required, for example, for debugging purposes. After you add a new NVA rule to enable a port, it remains active only for two hours. Simultaneously, adding another NVA rule restarts the timer, and now all the enabled ports remain active for two hours.

Note

- Security rules of NVAs are not configurable when the cloud gateway operations are in progress.
- The source IP address for Azure can only have /30, /31, or /32 as suffixes. Examples of the source IP address for Azure are 192.0.2.0/30, 192.0.2.0/31, 192.0.2.0/32.

Information About Azure ExpressRoute Connection to NVA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, Cisco SD-WAN Manager supports ExpressRoute connections from branch offices to NVAs through SD-WAN tunnels. Express route connections are private networks that offer high reliability, few latencies, and fast connections for data transfer.

For further details about Azure ExpressRoute Connection to NVA, see Alternative Azure Designs.

Information about Multiple Virtual Hubs in Each Region

Minimum supported release: Cisco vManage Release 20.11.1

Note This feature is supported on both Azure Cloud and Azure Government Cloud.

For organizations with thousands of sites connected to Azure in a single region, Microsoft supports creation of multiple cloud gateways, and up to eight virtual hubs for a single region.

For Cisco vManage Release 20.10.1 and earlier releases, the Azure Virtual WAN solution supports only a single virtual hub in a single region. From Cisco vManage Release 20.11.1, the solution supports multiple virtual hubs in each region.

The cloud gateway attachment to a virtual network is based on a load balancing algorithm. When you add a tag to the cloud gateway attachment, you can choose **Auto** which distributes the VNets based on the load balancing algorithm. When you create a new cloud gateway, you can choose to redistribute VNets to load balance the existing VNets among all the cloud gateways. You can only reassign VNets across cloud gateways when you choose the **Auto** VNet tag. You cannot reassign the dedicated VNet tags that are attached to cloud gateways.

Supported Devices for Azure Virtual WAN Integration

Supported Azure Instances

Azure virtual WAN integration supports the following Cisco Catalyst 8000V instances.

Table 69: SKU Scale Value and Azure Instance Types

SKU Scale Value	Instance Resources	Number of Instances	Supported From
2	2 CPU cores and 7 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a
4	4 CPU cores and 14 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

SKU Scale Value	Instance Resources	Number of Instances	Supported From
10	8 CPU cores and 32 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a
20	16 CPU cores and 64 GB memory	2	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a
40	16 CPU cores and 64 GB memory	3	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a
60	16 CPU cores and 64 GB memory	4	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a
80	16 CPU cores and 64 GB memory	5	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a



Note The Azure instance type for a specific SKU Scale is determined by Azure when you create the cloud gateway. To find out which instance type has been allocated, use the **show platform software system all** command in the CLI session of the Cisco Catalyst 8000V cloud gateway and look for the Instance Type field under Cloud Metadata.

Prerequisites for Azure Virtual WAN Integration

Prerequisites for Routing Traffic to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

Cisco Cloud OnRamp for Multicloud has been configured to operate together with a Microsoft Azure environment. See Microsoft Azure Virtual WAN Integration.

Prerequisites for Azure SKU Scaling, Audit, and Security Rules of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

- Cisco Cloud OnRamp for Multicloud must be configured to operate together with a Microsoft Azure environment. See Microsoft Azure Virtual WAN Integration.
- Azure cloud account details.
- Subscription to Azure Marketplace.

- Cisco SD-WAN Manager must be connected to the internet and must be able to communicate with Microsoft Azure to authenticate your Azure account.
- Cloud gateway must be operational.

Restrictions for Azure Virtual WAN Integration

Restrictions for Azure Virtual WAN Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

- Azure Virtual WAN hub architecture doesn't support segmentation.
- The VPNs you select for mapping to the VNets should not have overlapping IP address spaces.
- Because of VNet tagging, all the VPNs and VNets are visible to all the other VPNs and VNets.
- Only one virtual hub can be configured for each Azure region and for each resource group.
- Only one resource group is permitted on Cisco SD-WAN Manager.
- For inter-region hub-to-hub connectivity, all the virtual hubs must be part of the same Azure Virtual WAN.
- IPv6 is not supported.
- Azure virtual WAN hubs don't support trace route.
- Branches connected to the virtual WAN hub can only be assigned to the default route table of the virtual WAN hub.
- If no virtual WAN hub is created or discovered in an Azure region through Cisco SD-WAN Manager, the VNets in that region don't get mapped using VNet tags.
- For deploying the Cisco Catalyst 8000V Network Virtual Appliances (NVAs) in the Azure WAN hub, it is supported under one resource group and virtual WAN. You can not deploy Cisco Catalyst 8000V in different resource groups. After the Cisco Catalyst 8000V NVA deployment, by default is associated to that resource group and virtual WAN for subsequent deployments.

Restrictions for Routing Traffic to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

Routing local traffic to an Azure secure virtual hub operating with the Azure Firewall Manager may involve additional operating charges for your Azure environment. Check the terms of your Azure service.

Restrictions for Azure SKU Scaling, Audit, and Security Rules of Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

- The multicloud audit service cannot run while a cloud gateway is being created, edited, or deleted.
- The ability to change the SKU scale values and the audit feature, and the ability to open ports temporarily apply only to cloud gateways that are created in Cisco SD-WAN Manager using the multicloud. These features do not apply to the Network Virtual Appliances created directly on the Azure portal.

Restrictions for Multiple Virtual Hub per Region

Minimum supported release: Cisco vManage Release 20.11.1

A maximum of 8 virtual hubs can be created per region.

Use Cases for Azure Virtual WAN Integration

Use Cases for Routing Traffic Flow to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

- Routing traffic to a secured virtual hub or to a local firewall may be useful where it is desirable to apply the same firewall policy to all of the Azure-based and local internet traffic, using either an Azure-based firewall or a local firewall.
- Routing local traffic to a secured virtual hub may be useful if you do not want to set up a firewall on a local branch device.
- Routing Azure traffic to a local firewall may be useful if you do not want to set up a firewall in the Azure environment.

Use Cases for Azure SKU Scaling

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

You can configure the SKU Scale value for either better performance or better cost effectiveness of cloud gateway services. If the CPU load is above 75 percent, then you can configure a higher SKU Scale value, and if the CPU load is below 25 percent, you can configure a lower SKU Scale value.

Use Cases for Azure Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

If you are facing any connectivity or networking issues, then initiate an audit. The information provided by Azure audit helps in troubleshooting the networking issues.

Use Cases for Security Rules of NVAs

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Security rules configuration of NVAs allows you to enable a particular port.

Configure Azure Virtual WAN Integration

Configure Azure Virtual WAN Hubs

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

Use the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager to create Azure virtual WAN hubs to connect your Cisco Catalyst SD-WAN branches to the applications in your private networks or Host VNets. To configure an Azure virtual WAN hub, perform the following tasks in the order specified.

Configuration Prerequisites

You need the following to be able to configure Azure virtual WAN hubs using Cisco SD-WAN Manager.

- Azure cloud account details.
- Subscription to Azure Marketplace.
- Cisco SD-WAN Manager must have two Cisco Catalyst 8000V licenses that are free to use for creating the Azure Cloud Gateway.
- Cisco SD-WAN Manager must be connected to the Internet and must be able to communicate with Microsoft Azure to authenticate your Azure account.

Integrate Your Azure Cloud Account

Associate your Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Setup**, click **Associate Cloud Account**.
3. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
4. Enter the requested information:

Field	Description
Cloud Account Name	Enter a name for your Azure subscription.

Field	Description
Description (optional)	Enter a description for the account. This field is optional.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.
Tenant ID	Enter the ID of your Azure Active Directory (AD). To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use as part of this workflow.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret Key	Enter the password associated with the client ID.

5. Click **Add**.



Note If you are using multiple Azure subscriptions to discover the VNets or to create cloud gateways, you must add all the subscriptions that are under the same tenant as different Azure Accounts in **Cloud OnRamp for Multicloud Set up** > **Associate Cloud Account**.

Add and Manage Global Cloud Settings

1. On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.
2. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
3. To edit global settings, click **Edit**.
4. To add global settings, click **Add**.
5. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enable the **Enable Configuration Group** option to use configuration groups to configure devices in the multicloud workflow.
6. In the **Software Image** field, choose the software image of the WAN edge device to be used in the Azure Virtual Hub. This should be a preinstalled Cisco Catalyst 8000V image.



Note Choose the Cisco Catalyst 8000V image based on your Cisco SD-WAN Manager release. For Cisco SD-WAN Manager Release 20.n, choose the Cisco Catalyst 8000V image for Cisco IOS XE Release 17.n or earlier. For example, for Cisco SD-WAN Manager Release 20.5, you can choose an image corresponding to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or Cisco IOS XE Catalyst SD-WAN Release 17.5.1a. If a software image corresponding to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later is available among the preinstalled images, do not select such an image because it is not compatible with your Cisco SD-WAN Manager release.

7. In the **SKU Scale** field, from the drop-down list, choose a scale based on your capacity requirements.
8. In the **IP Subnet Pool** field, specify the IP subnet pool to be used for the Azure virtual WAN hub. A subnet pool needs prefixes between /16 and /24. You can use /16 prefix in the global settings and then overwrite the settings with /24 when you create a cloud gateway.



Note **IP Subnet Pool** from the global settings is used only when a virtual hub is not deployed in a given region. When a virtual hub is deployed in a region, this field is auto-populated from cloud and you cannot edit the values.

A single /24 subnet pool is able to support one cloud gateway only. You cannot modify the pool if other cloud gateways are already using the pool. Overlapping subnets are not allowed.

The IP subnet pool is meant for all Azure Virtual WAN Hubs inside an Azure Virtual WAN, one /24 prefix per Virtual WAN Hub. Ensure that you allocate enough /24 subnets for all the Virtual WAN Hubs you plan to create within the Virtual WAN. If a Virtual WAN Hub is already created in Microsoft Azure, you can discover it through Cisco SD-WAN Manager and use the existing subnet pool for the discovered hub.

9. In the **Autonomous System Number** field, specify the ASN to be used by the cloud gateway for eBGP peering with the virtual hub.



Attention This value cannot be modified after a cloud gateway has been created.

10. For the **Push Monitoring Metrics to Azure** field, choose **Enabled** or **Disabled**. If you choose **Enabled**, the cloud gateway metrics associated with your Azure subscription are sent to the Microsoft Azure Monitoring Service portal periodically. These metrics are sent in a format prescribed by Microsoft Azure for all NVA vendors.



Important

- There is a separate cost associated with using the Azure Monitor Service for processing and monitoring the data sent through Cisco SD-WAN Manager. Refer to Microsoft Azure documentation for information on billing and conditions of use.
- It is the responsibility of managed service providers to provide notice to and obtain any necessary legal rights and permissions from end users regarding the collection and processing of their telemetry data.

11. From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can enable or disable the **Advertise Default route to Azure Virtual Hub** field. By default, this field is **Disabled**. If you click **Enabled**, the internet traffic from the virtual network is redirected through Cisco Catalyst SD-WAN branches.
12. From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can enable or disable the **Enable Periodic Audit** field by clicking **Enabled** or **Disabled**.

    If you the enable periodic audit, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.
13. From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can enable or disable the **Enable Auto Correct** field by clicking **Enabled** or **Disabled**. If you enable the auto correct option, after every periodic audit is triggered, all the recoverable issues that are discovered are auto corrected.
14. Click **Add** or **Update**.

Create and Manage Cloud Gateways

Creation of cloud gateways involves the instantiation or discovery of Azure Virtual WAN Hub and two Cisco Catalyst 8000V instances within the hub.

Note If you have used the Azure portal to provision Cisco Catalyst 8000V instances, and created an Azure Virtual WAN and Azure Virtual WAN Hub using the Azure portal, you can also discover them using the procedure below.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Manage**, click **Create Cloud Gateway**.
3. In the **Cloud Provider** field, choose **Microsoft Azure** from the drop-down list.
4. In the **Cloud Gateway Name** field, enter the name of your cloud gateway.

Note If you have created an Azure Virtual WAN Hub using the Azure portal, ensure that you enter the exact virtual hub name in this field. This ensures that the resources associated with the hub are discovered. The associated Azure Virtual WAN and Azure Virtual WAN Hub then become available for you to choose from in the **Virtual WAN** and **Virtual Hub** fields. The associated NVAs also autopopulate in the **UUID** field.

5. (Optional) In the **Description** field, enter a description for the cloud gateway.
6. In the **Account Name** field, choose your Azure account name from the drop-down list.
7. In the **Region** field, choose an Azure region from the drop-down list.
8. (From Cisco Catalyst SD-WAN Manager Release 20.13.1, applies only if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for Azure cloud gateway) From the **Configuration Group** drop-down list, perform one of these actions:
   - Choose a configuration group.

- To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list.

The configuration group that you choose is used to configure devices in the multicloud workflow.

Note The **Configuration Group** drop-down list includes only configuration groups that you create as described in this step. It does not include other configuration groups that have been created in Cisco Catalyst SD-WAN. The configuration groups in this drop-down list include the options that are needed for this provider.

For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups.

9. In the **Resource Group** field, either choose a resource group from the drop-down list, or choose **Create New**.

Note If you choose to create a new Resource Group, you would also need to create a new Azure Virtual WAN and an Azure Virtual WAN hub in the next two fields.

10. In the **Virtual WAN** field, choose an Azure Virtual WAN from the drop-down list. Alternatively, click **Create New** to create a new Azure Virtual WAN.

11. In the **Virtual HUB** field, choose an Azure Virtual WAN Hub from the drop-down list. Alternatively, click **Create New** to create a new Azure Virtual WAN Hub.

    (Minimum supported release: Cisco vManage Release 20.11.1) When you select the **Region**, **Resource Group**, and **Virtual WAN**, the **Azure Virtual WAN Hub** field displays **Create a new vHub using Cloud Gateway Name**. From the drop-down list, select the discovered virtual hubs.

    The virtual hubs are discovered on Cisco SD-WAN Manager in two ways:

    - Virtual hubs with Network Virtual Appliances (NVAs) created on the Azure portal.
    - Virtual hubs created in the Azure portal and discovered by Cisco SD-WAN Manager. You can then add the NVAs to the virtual hubs in Cisco SD-WAN Manager.

12. (Minimum release: Cisco Catalyst SD-WAN Manager Release 20.13.1) From the **Solution Type** drop-down list, choose a virtual appliance that you want to deploy:

    - Choose **vHub with NVA** to create a network virtual appliance (NVA) in vHub with Catalyst 8000V instances. Choose this option to deploy Cisco SD-WAN devices in controller mode.
    - Choose **vHub with VPN** to create a VPN gateway in vHub, which is a bridge for on-premises devices to enter cloud resources. Choose this option to deploy Cisco SD-Routing devices in autonomous mode.

13. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.

14. In the **Settings** field, choose one of the following:

- **Default** - The default values of IP subnet pool, image version, and SKU Scale size are retrieved from global settings.
- **Customized** - you can override the global settings with this option. This option is applicable only for the newly created cloud gateway.

(Minimum supported release: Cisco vManage Release 20.10.1)

In the **Instance Setting** area, the following fields are auto-populated with the configurations from the global settings only when you onboard the virtual hubs with Cisco Catalyst 8000V created on Azure portal to Cisco SD-WAN Manager:

- **Software Image**
- **SKU Scale**
- **IP Subnet Pool**
- **UUID (specify 2)**



Note When the cloud gateways are onboarded on Cisco SD-WAN Manager, without the NVAs, the **IP Subnet Pool** and **UUID (specify 2)** fields are auto-populated.

Routers in NVA get IP addresses over DHCP in the Azure portal. Cisco SD-WAN Manager learns the IP addresses assigned to the routers via API's.

You can override the global settings by selecting the options in the drop-down list.

15. From Cisco Catalyst SD-WAN Manager Release 20.13.1, applies only if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for Azure cloud gateway) In the **Configuration Group**, choose the name of the configuration group that is to be used to create the cloud gateway, or create a new configuration group.

(

16. In the **UUID (specify 2)** field, choose two Cisco Catalyst 8000V licenses from the drop-down list.



Note From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

17. (Minimum release: Cisco vManage Release 20.10.1) In the **Multi-Region Fabric Settings** area, for **MRF Role**, choose **Border** or **Edge**.

    This option is available only when Multi-Region Fabric is enabled.

18. Click **Add**.



Note It can take up to 40 minutes for your Azure Virtual WAN hub to be created and for the Cisco Catalyst 8000V instances to be provisioned inside the virtual hub.

Note Once the creation of the Azure Virtual WAN Hub is complete, you have the option to convert it into a secured Azure Virtual WAN Hub. However, this configuration can only be completed through the Microsoft Azure portal. See Microsoft Azure documentation for more information.

Note You can simultaneously create Azure cloud gateways in different regions.

- Before creating multiple cloud gateways in different regions, create the resource group, virtual WAN, and storage account for the first cloud gateway.
- Before creating multiple cloud gateways in the same region, create the virtual hub for the first cloud gateway in the region.
- You need to have blob access to create a storage account in Azure for the Cloud OnRamp for Multicloud. Blob access is required while creating cloud gateways and modifying scale operations on the Cisco Catalyst 8000V devices.

Note The Cloud OnRamp for Multicloud workflow supports up to eight virtual hubs in each Azure region. You can deploy two cloud gateway Network Virtual Appliances (NVAs) in each virtual hub.

Discover Host VNets and Create Tags

After you create an Azure virtual hub, you can discover your host VNets in the region of the virtual hub.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Discover** workflow, click **Host Private Networks**.
3. In the **Cloud Provider** field, choose **Microsoft Azure**.

   A list of your host VNets displays in a table with the following columns: Cloud Region, Account Name, VNET Tag, Cloud Gateway Attachment, Account ID, Resource Group, and VNet Name.
4. Click the **Tag Actions** drop-down list to choose any of the following:
   - **Add Tag:** Create a tag for a VNet or a group of VNets.

     (Minimum supported release: Cisco vManage Release 20.11.1) You can choose the **Cloud Gateway Attachment** as **Auto** or map with an existing cloud gateway.
   - **Edit Tag:** Change the existing tag of a selected VNet.

     (Minimum supported release: Cisco vManage Release 20.11.1) You can choose the **Cloud Gateway Attachment** from the **Edit Tag**. The **Auto** option is automatically selected, if you choose not to make a selection or if the cloud gateway is not yet created in that region. The **Auto** option is based on a load balancing algorithm. For VNets with the **Auto** option selected, the cloud gateway attachments are selected during mapping and not when the tag is created.
   - **Delete Tag:** Delete the tag for the selected VNet.

Map VNets Tags and Branch Network VPNs

To enable VNet to VPN mapping, you select a set of VNets in one or multiple Azure regions and define a tag. You then select the service VPNs that you want to map the VNets to using the same tags. Only a single set of VNets can be mapped to a single set of branch offices. All selected VNets are visible to all selected VPNs and vice versa. One service VPN can be mapped to a single or multiple tags. Multiple VNets could have the same tag. Mapping is automatically realized when a cloud gateway exists in the same region or when tagging operations take place.



Note The VPNs selected to be mapped to VNet tags must not have overlapping IP addresses. This is because segmentation is not supported in Microsoft Azure Virtual WAN.

To edit the VNet-VPN mapping for your Cisco Catalyst SD-WAN networks, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under, **Intent Management** click **Connectivity**.
3. To define the intent, click **Edit**.
4. Choose the cells that correspond to a VPN and the VNet tags associated with it, and click **Save**.

The **Intent Management - Connectivity** window displays the connectivity status between the branch VPNs and the VNet tags they are mapped to. A legend is available at the top of the screen to help you understand the various statuses. Click any of the cells in the matrix displayed to get a more detailed status information, such as, Mapped, Unmapped, and Outstanding mapping.

Rebalance VNets

Minimum supported release: Cisco vManage Release 20.11.1

You can choose to redistribute VNets to load balance the existing VNets among all the cloud gateways in a region for a given tag at any time. You can reassign only the VNets with **Auto** option selected across cloud gateways. The VNets assignment is based on a load-balancing algorithm. As the rebalancing involves detachment and re-attachments of VNETs to cloud gateways, traffic disruption may occur. After rebalancing the VNets, you can view the revised mapping of VNETs to cloud gateways on the tagging page.



Note You cannot rebalance VNets when:

- Create, edit, or delete of Cloud gateway is in progress.
- Mapping of VNets is in progress.
- Audit is in progress.

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Cloud OnRamp for Multicloud**.
2. In **Intent Management** workflow, click **Rebalance VNETS (Azure/GovCloud)**
3. In the **Cloud Provider** field, choose **Microsoft Azure**.

4. In the **Region** field, choose an Azure region from the drop-down list.
5. In the **Tag Name** field, choose a tag from the drop-down list.
6. Click **Rebalance**.

Configure an Azure Virtual WAN Hub Through the Azure Portal

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

Note The end-to-end configuration of Azure virtual WAN hub can be done using Cisco SD-WAN Manager. Alternatively, you can use the Azure portal to create resource groups, virtual WAN, and virtual WAN hub, and then return to Cisco SD-WAN Manager to discover the infrastructure you created using the Azure portal, and then create VNet tags and map them to your service VPNs.

Configuration Workflow

Task	Description
Task 1	From the Cisco SD-WAN Manager menu, select two Cisco Catalyst 8000V instances that are free to use for the Azure virtual WAN hub. Next, generate and download a bootstrap configuration file for these instances.
Task 2	In the Azure portal, create a managed identity and a custom role with the necessary permissions. Assign the role to the managed identity in the resource group.
Task 3	In the Azure portal, create a virtual WAN hub and associate the Cisco Catalyst 8000V instances with the virtual WAN hub you create.
Task 4	In the Azure portal, create NVAs for Cisco Catalyst 8000V using the bootstrap configuration file generated in Cisco SD-WAN Manager.
Task 5	In Cisco SD-WAN Manager, discover the infrastructure you created in the Azure portal. As part of this discovery, the NVAs created in the Azure Virtual WAN Hub are brought up.
Task 6	In Cisco SD-WAN Manager, configure connectivity between the host VNets and service VPNs by mapping VNet tags.

Note Any configuration done using the Azure portal is out of scope of this document. However, we've provided links to Azure documentation to help you complete the configuration using the Azure portal.

Task 1. Generate Bootstrap Configuration for Cisco Catalyst 8000V

Prerequisite: You must have licenses available in Cisco SD-WAN Manager for two Cisco Catalyst 8000V instances before proceeding with the next steps.

To generate bootstrap configuration for Cisco Catalyst 8000V using configuration groups, ensure that you have enabled the **Enable Configuration Group** option in the Azure global settings and follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** on the Cloud OnRamp for Multicloud dashboard. Click **Add gateway** and proceed to configure the parameters to create the gateway.
3. In the **Configuration groups** field, create a new configuration group by choosing **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**.
4. Once you create the configuration group, click **Cancel** to abort the cloud gateway creation workflow.
5. Associate the Cisco Catalyst 8000V devices to the configuration group that you created in Step 3. For more information see, Add Devices to a Configuration Group.
6. Deploy a Configuration Group.
7. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
8. Locate the devices you updated and for each of the devices, click **...**. Choose **Generate Bootstrap Configuration** from the options.
9. On the **Generate Bootstrap Configuration** dialog box, deselect **Include Default Root Certificate** , and click **OK**.

   You can see the **Include Default Root Certificate** option only if you have an enterprise certificate for Cisco SD-WAN Manager.
10. On the dialog box, click **Download**.

To generate bootstrap configuration for Cisco Catalyst 8000V using templates, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

3. From the **Template Type** drop-down list, choose **Default**.

   A list of default templates is displayed.
4. For the desired row in **Default_Azure_vWAN_C8000V_Template_V01**, click **...** and choose **Attach Devices**.
5. From the list of **Available Devices**, choose two Cisco Catalyst 8000V instances and click **Attach**.

   On the next screen, you'll see the devices that you attached to the device template.
6. On the Device Templates screen, for each of the device rows, click **...** and choose **Update Device Template**.

7. For each of the devices, enter the requested information: Host Name, System IP, and Site ID. Click **Update**.
8. Click **Next**. On the **Configure Devices** dialog box, check the check-box and click **OK**.

   The **Task View** screen opens. It takes a few minutes for the device information to be updated. When the status column shows the status as **Done - Complete**, it indicates that the device information has been updated.
9. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
10. Locate the devices you updated and for each of the devices, click **...**. Choose **Generate Bootstrap Configuration** from the options.
11. On the **Generate Bootstrap Configuration** dialog box, deselect **Include Default Root Certificate** , and click **OK**.
12. On the dialog box, click **Download**.

Task 2. Create a Managed Identity and a Custom Role

In the Azure portal, complete the following:

1. Create managed identities.
2. Create a custom role.
3. Assign the custom role to the managed identity for a resource group hosting the virtual WAN Hub.

Task 3. Create Azure Virtual WAN Hub

The steps in this section are performed in the Azure portal. We have provided links to Azure documentation for completing these step. You need an Azure subscription and login credentials to perform the steps in this section.

In the Azure portal, complete the following:

1. Create resource groups.
2. Create a virtual WAN.
3. Create a virtual WAN hub.

Next step: In the virtual hub, create a Network Virtual Appliance (NVA) for your Cisco Catalyst 8000V instances. The procedure to create NVAs may differ for various NVA partners. Therefore, we've provided information specific to Cisco Catalyst 8000V in the next section.

Task 4. Create NVA for Cisco Catalyst 8000V

1. In the Azure portal, search for **Cisco Cloud vWAN Application** in the search box and click the result under Marketplace.
2. The **Cisco Cloud vWAN Application** page opens. Click **Create**.

   Enter the requested details and click **Next: Cisco SD-WAN Cloud Gateway**.
3. Click **NVA Application Settings**.
   a. Click **Add**.

b. Check the check box to select the managed identity created in Task 2.

4. Enter the requested details. The details you enter on this screen are similar to the Cloud Global Settings screen in Cisco SD-WAN Manager.
   a. **Virtual WAN:** Choose the virtual WAN your created from the drop-down list.
   b. **Virtual WAN Hubs:** When you choose a virtual WAN, all the virtual hubs in that WAN are shown in the drop-down list. Choose the virtual WAN hub you want to use for this procedure.
   c. **Scale Unit:**
   d. **Cisco Version:** Enter the software version for the Cisco Catalyst 8000V instances.
   e. **BGP ASN to peer with Azure Router Service:** This is the number that the NVA uses.
   f. **Cisco SDWAN Cloud Gateway Name:** Enter a name for the cloud gateway.
   g. **Upload the Bootstrap configuration File that was generated:** Using this field, navigate to the bootstrap configuration files you downloaded for Cisco Catalyst 8000V from Cisco SD-WAN Manager.

Note Ensure that you select both the bootstrap configuration files at this step.

5. Click **Next** and retain the default values.
6. Check the check box to agree to the terms and conditions. Click **Create**.

   When the deployment is complete, two Cisco Catalyst 8000V instances are provisioned inside the virtual hub. When they come up, they are also connected to Cisco SD-WAN Manager.

In Cisco SD-WAN Manager, on the main dashboard, click the upward arrow next to Devices. If your deployment through the Azure portal is successful, you'll see the two Cisco Catalyst 8000V instances show as reachable.

Task 5. Discover NVAs in Cisco SD-WAN Manager

Prerequisite: To discover NVAs in Cisco SD-WAN Manager, your Azure account should be added in Cisco SD-WAN Manager. If you haven't already associated your Azure account with Cisco SD-WAN Manager, see Integrate Your Azure Cloud Account, on page 357.

To discover your NVAs or the Cisco Catalyst 8000V you configured using the Azure portal, follow the steps outlined in Create and Manage Cloud Gateways, on page 360.

Task 6. Configure Connectivity Between VNets and VPNs

To configure VNet to VPN tagging, you first need to discover the host VNets in your Azure regions and create tags and then map these tags to connect the VNets and your branch networks or VPNs.

Configure Routing of Traffic Flow to a Secured Virtual Hub or a Local Firewall

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

Route Local Outgoing Traffic Flow to an Azure Secured Virtual Hub

Before You Begin

- Configure integration of your Azure Virtual WAN hub with Cisco Catalyst SD-WAN. For information about this, see Azure Virtual WAN Hub Integration with Cisco SD-WAN.
- Configure a firewall in the Azure environment, including the desired firewall policy.

Route Local Outgoing Traffic Flow to an Azure Secured Virtual Hub

To configure a branch router to route outgoing internet traffic to an Azure secured virtual hub, perform these steps.

1. On the local branch router, verify that the branch router does not have a static default route configured for direct internet access (DIA) from the branch.

   On the local branch router, use the **show ip route vrf** *vrf-number* command to verify that the static default route is not configured for the service side VPN.

2. On the local branch router, use the **show ip route vrf** *vrf-number* command to verify that internet traffic from the local branch router has been routed to the Azure firewall using the VRF that you have configured for communication between the local branch router and Azure. In the command output, look for the IP addresses associated with the default route, which is represented as 0.0.0.0. The IP addresses must correspond to the cloud gateways operating in the Azure hub where the Azure firewall is enabled.

   The following example uses VRF 100. In the example, only a portion of the command output is shown. The IP addresses that correspond to the cloud gateways operating in the Azure hub are 209.165.201.1 and 209.165.201.2.

   ```
   Device# show ip route vrf 100

   ...
   m*    0.0.0.0/0 [251/0] via 209.165.201.1, 21:06:00, Sdwan-system-intf
                   [251/0] via 209.165.201.2, 21:06:00, Sdwan-system-intf
   ...
   ```

3. In the Azure environment, configure internet traffic to be routed through the Azure firewall.

Route Azure Outgoing Traffic Flow to a Local Branch Router

Before You Begin

- Configure integration of your Azure Virtual WAN hub with Cisco Catalyst SD-WAN. For information about this, see Azure Virtual WAN Hub Integration with Cisco SD-WAN.
- Configure a firewall on the local branch router, including the desired firewall policy.

Route Azure Outgoing Traffic Flow to a Local Branch Router

To configure Azure to route outgoing internet traffic to a local branch router firewall, perform these steps.

1. In Cisco SD-WAN Manager, use the CLI template for the local branch router to add the following commands to the configuration. This advertises the local router as the default route for the Azure

environment, causing the Azure virtual network to route its outgoing internet traffic to the branch router. Note that 0.0.0.0 represents the default route.

```
address-family ipv4 vrf branch-router-vpn-id
   advertise connected
   advertise static
   advertise network 0.0.0.0/0
```

Only traffic in the specified VPN is directed to the branch router. For information about how VPNs map the connectivity between Cisco Catalyst SD-WAN and Azure, see How Virtual WAN Hub Integration Works.

The following example directs Azure traffic in VPN 100 to the branch router:

```
address-family ipv4 vrf 100
   advertise connected
   advertise static
   advertise network 0.0.0.0/0
```

2. In the Azure environment, verify that the traffic is routed to the local branch router. View the routing table and verify that the following appears:

   Prefix: 0.0.0.0/0
   Next Hop Type: VPN_S2S_GATEWAY

Configure SKU Scale Value

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to configure SKU Scale value:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Cloud Gateways** with a table displaying the list of cloud gateways with cloud account name, ID, cloud type, and other information, is displayed.
3. Click **...** adjacent to the corresponding cloud gateway, and choose **Edit**.
4. From the **SKU Scale** drop-down list, choose a value. .

Note Only SKU Scale values **2**, **4**, and **10** are supported.

5. Click **Update**.

Initiate On-Demand Audit

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

This is a user-invoked audit. Follow these steps to initiate an on-demand audit:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

2. Click **Audit** under **Intent Management**.
3. For the **Cloud Provider** drop-down list, choose **Microsoft Azure**.

   The window displays the status for various Microsoft Azure objects. If the status is **In Sync** for any of the objects, it means the object is free from errors. If the status of an object is **Out of Sync**, it means that there are discrepancies between the object details available on Cisco SD-WAN Manager and the details available on the Azure database.
4. If the status is **Out of Sync** for any of the objects, click **Fix Sync issues**. This option resolves recoverable errors, if any, and opens a window that displays the status activity log.

   If the status of an object still shows **Out of Sync**, it means that it is an error that requires manual intervention.

Note The multicloud audit service does not run while other cloud operations are in progress.

Enable Periodic Audit

The following steps describe the procedure to enable periodic audit:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Setup** area, click **Cloud Global Settings**.
3. To enable or disable the **Enable Periodic Audit** field, click **Enabled** or **Disabled**.

   If you click **Enabled**, Cisco SD-WAN Manager triggers an automatic audit every two hours. This automatic audit takes place in the background, and a discrepancies report is generated.

   For examples on audit discrepancies and resolutions, see Examples of Audit Discrepancies.
4. Click **Update**.

Configure Security Rules of NVAs

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to configure security rules for NVA:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Create Cloud Gateways** window with a table displaying the list of cloud gateways with cloud account name, ID, cloud type, and other information is displayed.
3. Click **...** adjacent to the corresponding cloud gateway, and choose **Add/Edit Security Rules**.

   The **Add/Edit Security Rules** window is displayed.

   a. To add a new security rule, click **Add Security Rule** and provide the following details:

Table 70: Parameters Table

Parameter	Description
Port Number	Provide the port range.
IPv4 Source Address	Provide the IP address.

b. Click **Add**.

c. (Optional) To edit a security rule, click the pencil icon.

d. (Optional) To delete a security rule, click the delete icon.

4. Click **Update**.

Note All the security rules are active only for two hours.

Verify Azure Virtual WAN Integration

View, Edit, or Delete a Cloud Gateway

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Cloud OnRamp for Multicloud**.
2. Click **Cloud**.
3. Under **Manage**, click **Gateway Management**.

   Existing cloud gateway details are summarized in a table.
4. In the table, click **…** for the desired Cloud Gateway.
   - To view more information about the cloud gateway, click **View**.
   - To edit the cloud gateway description, click **Edit**.
   - To delete the cloud gateway, click **Delete** and confirm that you wish to delete the gateway.

     (Minimum supported release: Cisco vManage Release 20.11.1) If you delete a cloud gateway, the attached VNets move to other selected cloud gateways in the same region based on a load balancing algorithm and the VNets are marked as **Auto**.

Verify Azure SKU Scale Value Update

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to verify the Azure SKU scale value update:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Create Cloud Gateways** window is displayed. A table displays the list of cloud gateways with cloud account name, ID, cloud type, and other information.
3. Click **...** adjacent to the corresponding cloud gateway, and choose **View**.

   The changed SKU value appears on the **View Cloud Gateway** window.

Verify Security Rule for Network Virtual Appliances

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Follow these steps to verify a security rule created for NVA:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Gateway Management** under **Manage**.

   The **Create Cloud Gateways** window with a table displaying the list of cloud gateways with cloud account name, ID, cloud type, and other information is displayed.
3. For the desired cloud gateway, click **...** and choose **Add/Edit Security Rules**.

   The **Add/Edit Security Rules** window is displayed along with one of the following statuses of the updated security:

   - **Successful**
   - **In-progress: Check the status after sometime.**
   - **Failed: Recreate the security rule.**

Monitor Azure Virtual WAN Integration Using Cisco SD-WAN Manager

Monitor Azure Virtual WAN Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco vManage Release 20.4.1

NVA Connectivity

When you create a new cloud gateway, you can verify the creation and reachability of the Cisco Catalyst 8000V instances provisioned inside the Azure virtual WAN hub. To view whether these instances are configured successfully and are reachable, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

Cisco SD-WAN Manager Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. Under **WAN Edge**, click the upward arrow next to the number displayed. The number represents the WAN Edge devices available.
3. In the table that displays in the pop-up window, look for the Cisco Catalyst 8000V instances you chose while creating a cloud gateway. If your cloud gateway configuration was successful, the instances should appear in the table and show as reachable.

Monitor NVA Data Using Microsoft Azure Monitor Service

In Cisco SD-WAN Manager, you can enable sending metrics to the Azure portal using the **Cloud OnRamp for Multicloud** > **Cloud Global Settings** window.

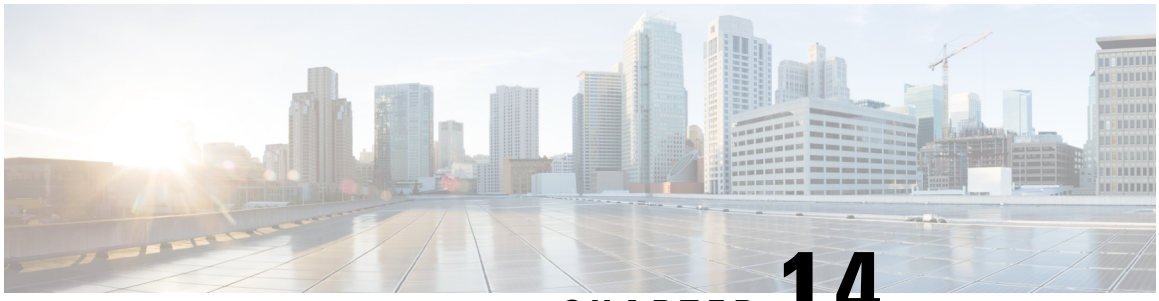
If you enable the **Push Monitoring Metrics to Azure** option, data about all the Cloud Gateways associated with the Azure account, that you have integrated with Cisco SD-WAN Manager, is sent to the Azure Monitor service.

For details about the Azure Monitoring service, see Azure documentation.



Important

- There is a separate cost associated with using the Azure Monitor Service for processing and monitoring the data sent through Cisco SD-WAN Manager. Refer to Microsoft Azure documentation for information on billing and conditions of use.
- It is the responsibility of managed service providers to provide notice to and obtain any necessary legal rights and permissions from end users regarding the collection and processing of their telemetry data.



CHAPTER 14

Microsoft Azure for US Government Integration

Table 71: Feature History

Feature Name	Release Information	Description
Support for the Azure for US Government Cloud with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With the integration of the Azure for US Government cloud with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, you can move and store your highly sensitive workloads in an isolated cloud that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements of the U.S. government and its customers. All of the same features that are available for the Azure integration with Virtual WAN are also available with the Azure for US Government cloud.
Configure Devices for Azure for US Government Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for Azure for US Government.

- Information About Azure for US Government Integration, on page 376
- Supported Devices for Azure for US Government, on page 376
- Prerequisites for Azure for US Government Integration, on page 377
- Restrictions for Azure for US Government Integration, on page 377
- Use Case for Azure for US Government Integration, on page 377
- Configure Azure for US Government, on page 377
- Monitor Azure for US Government Integration, on page 378

Information About Azure for US Government Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

This feature adds the Azure for US Government cloud to Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, allowing you to move and store your highly sensitive workloads in the Azure for US Government cloud.

The following are examples of highly sensitive workloads that you can store in the Azure for US Government cloud:

- Controller Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export data

The same features that are available for the Azure Virtual WAN integration are also available with the Azure for US Government integration. Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch connectivity through Azure.

For more information on the Azure for US Government cloud, see the Azure for US Government documentation.

Configure Azure for US Government as part of Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud in Cisco SD-WAN Manager.

Benefits of Azure for US Government Integration

- Allows you to store your highly sensitive workloads in the Azure for US Government cloud as part of Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud in Cisco SD-WAN Manager
- Supports the same features and workflow as for the Azure Virtual WAN integration in Cisco SD-WAN Manager
- Provides an isolated instance of Azure for storing data exclusively for U.S. government workloads
- Provides increased security with data centers and networks located in the U.S
- Limits potential access to sensitive data to only screened U.S. personnel
- Includes support for region pairing for providing geo-redundant storage

  For more information on region pairing, see the Microsoft Azure documentation.

Supported Devices for Azure for US Government

For more information on the supported devices for Azure for US Government, see Supported Azure Instances.

Prerequisites for Azure for US Government Integration

For more information on the prerequisites for Azure for US Government integration, see Prerequisites for Azure Virtual WAN Integration.

Restrictions for Azure for US Government Integration

- No support for creating a Network Virtual Appliance (NVA) from the Azure portal.
- No telemetry support for Azure for US Government.

Use Case for Azure for US Government Integration

Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud with Azure for US Government cloud allows you to safely move and store your highly sensitive data in the Azure for US Government cloud. The Azure for US Government cloud is an isolated cloud dedicated to the workloads of the U.S. government and its customers.

The following are examples of sensitive data that you can store in the Azure for US Government cloud:

- Controller Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export data

Configure Azure for US Government

The workflow for configuring Azure for US Government integration is the same as the workflow as for the Azure Virtual WAN integration.

1. Associate your Azure for US Government account with Cisco SD-WAN Manager.

   For more information on associating your Azure for US Government account, see Integrate Your Azure Cloud Account.

2. Add and manage your cloud global settings.

   For more information on configuring cloud global settings for Azure for US Government, see Integrate Your Azure Cloud Account.

3. Create and manage your cloud gateways.

   For more information on creating and managing your cloud gateways, see Create and Manage Cloud Gateways.

4. Discover your host virtual network (VNets) and create tags.

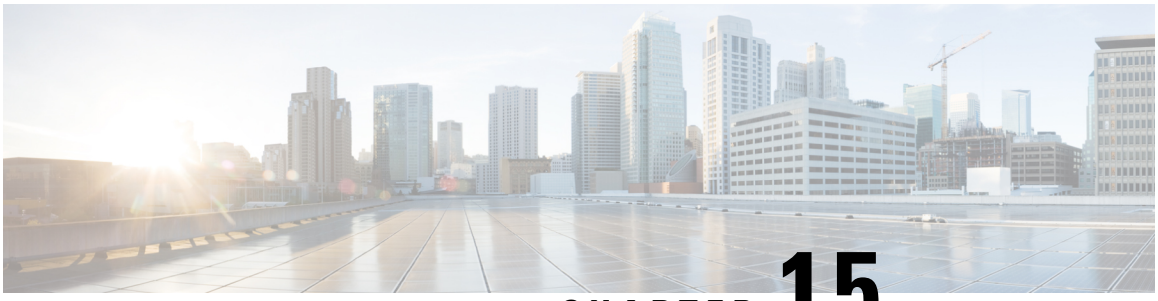
   For more information on discovering host VNets and creating tags, see Discover Host VNets and Create Tags.

5. Map your VNet tags and branch network VPNs.

   For more information on mapping your VNets and branch network VPNs, see Map VNet Tags and Branch Network VPNs.

Monitor Azure for US Government Integration

For more information on monitoring the Azure for US Government integration, see Monitor Azure Virtual WAN Integration.



CHAPTER 15

Google Cloud Integration

Table 72: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Cloud Gateway with Google Cloud	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows branch sites to access workloads running in the Google Cloud. It also allows branch sites to send and receive traffic across different regions and sites through Google Cloud's global network. As part of the solution, cloud gateways are instantiated in different regions. Cloud gateways consist of a pair of Cisco Catalyst 8000V instances with their interfaces anchored in three different VPCs. This feature supports site-to-cloud and site-to-site connectivity.

Feature Name	Release Information	Description
Cisco SD-WAN and Google Service Directory Integration and Support for Cloud State Audit and Cloud Resource Inventory	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	With the integration of Google Service Directory with the Cisco Catalyst SD-WAN solution, you can discover your applications in the Google cloud using Cisco SD-WAN Manager. You can use the discovered applications to define application-aware routing policies in Cisco SD-WAN Manager. The Audit feature in Cisco SD-WAN Manager is now extended to Google Cloud integration. Use this option to ensure that the states of the objects in Google Cloud stay in sync with Cisco SD-WAN Manager state. Cloud Resource Inventory in Cisco SD-WAN Manager retrieves a detailed list of your cloud objects, their identifiers, the timestamps when such objects were created, and so on.
Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway	Cisco vManage Release 20.9.1	With this feature, you can deploy between two and eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region. In earlier releases, you can deploy exactly two Cisco Catalyst 8000V instances as part of a cloud gateway, with each instance deployed in a different zone of a region.

Feature Name	Release Information	Description
Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways	Cisco vManage Release 20.9.1	With this feature, you can configure some cloud gateways to support site-to-site and site-to-cloud connectivity, and other cloud gateways to support only site-to-cloud connectivity. This configuration flexibility is particularly beneficial in some Google Cloud regions that do not yet support site-to-site connectivity. In earlier releases, connectivity type is a global configuration. You configure all the cloud gateways to support site-to-site and site-to-cloud connectivity, or to support only site-to-cloud connectivity.

- Supported Platforms and Instances, on page 381
- Limitations and Restrictions, on page 382
- Overview of Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud, on page 383
- Google Service Directory Integration and Lookup, on page 384
- Connectivity Models, on page 385
- Configure Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud, on page 387
- Service Directory Lookup and Traffic Policies with Discovered Apps, on page 394
- Monitor Connectivity, on page 397
- Audit, on page 397
- View Cloud Resource Inventory, on page 399

Supported Platforms and Instances

Supported Platform

- Cisco Catalyst 8000V

Supported Instances for Google Cloud

- N1-standard-8
- N1-standard-4

Limitations and Restrictions

- Google Network Connectivity Center location support depends on Google offerings. For information on supported locations, see the Google Cloud documentation for information about Google Network Connectivity Center locations.
- Change in service types (standard or premium) is only applicable to cloud gateways that are created after the change only. The change doesn't apply to cloud gateways that are already created.
- Only one service account is supported per Google Cloud project.
- Only one cloud gateway is supported per Google region.
- You can’t create new cloud gateways if the following are in progress:
  - creation or deletion of a cloud gateway
  - creation or mapping of tags
- You can’t edit settings for cloud gateways that are already created.
- If the first cloud gateway has already been created, you can't change the following cloud global settings:
  - IP Subnet Pool
  - Cloud Gateway BGP ASN Offset
- Workload VPC subnets can’t have overlapping IP address spaces.
- For site-to-site connectivity, you must configure a VRF and a centralized control policy to enable the branch-to-site traffic to go through Google Cloud's global network. If there’s failure in Google Cloud's global network tunnel, traffic is expected to be dropped.
- For site-to-cloud connectivity, only one VPN can be mapped to one or more tags.
- When a VPN is mapped to one or more tags, ensure that the combined number of VPCs under such tags don't exceed the VPC peering limit specified by Google Cloud. Intra-tag and tag-to-tag connectivity relies on VPC peering, therefore, the number of VPC peering relations that come into effect because of the intra-tag and tag-to-tag mapping shouldn't exceed VPC peering limit specified by Google Cloud. The default VPC peering limit is 25. Contact Google Cloud support to get this limit increased. See the Google Cloud documentation for information about Google VPC Peering limits.
- Tag-to-tag mapping is always bidirectional.
- For VPN-to-tag mapping for site-to-cloud connectivity, the number of prefixes should not exceed the maximum number of custom route advertisements per BGP session by Google cloud region, which is 200.
- By default, 20 Google Cloud routers are available per project. Site-to-cloud connectivity requires two Google Cloud routers. If site-to-site connectivity is enabled, two additional Google Cloud routers are required per cloud gateway. Therefore, with the default Google Cloud router quota availability, keeping site-to-site functionality disabled, you can create 10 cloud gateways for site-to-cloud connectivity. If you enable site-to-site connectivity as well, a maximum of five cloud gateway can be created. If you require additional Google Cloud routers for more cloud gateway instantiation, request for increase in your Google Cloud router quota through the Google Cloud portal.

- The dynamic routes learnt from workload VPCs at the site-to-cloud transit VPC are not further advertised to the BGP session with Cisco Catalyst 8000V instances in the cloud gateway. Therefore, these dynamic routes are not visible to Cisco Catalyst SD-WAN edge devices.
- IPv6 network addresses are not supported.
- The transit VPC hub in Network Connectivity Center can be deleted only if all the cloud gateways in a Google region are deleted.
- Transport location (TLOC) color **private1** is used only for site-to-site communication. Therefore, you should not use it for other interfaces.
- If you upgraded Cisco SD-WAN Manager from an earlier version to Cisco IOS XE Catalyst SD-WAN Release 17.18.1a or later with pre-existing cloud gateways, the existing WAN, S2C, S2S, and IC VPCs might have an MTU of 1460 bytes. Because an N4 CGW requires an MTU of 1500 bytes, the cloud gateways rejects the bootstrap file and fails to come up. You must update the MTU of all applicable VPCs to 1500 bytes using the GCP CLI before creating an N4 CGW.

  When you create a new cloud gateway on Cisco IOS XE Catalyst SD-WAN Release 17.18.1a or later, the workflow automatically provisions VPCs with an MTU of 1500 bytes by default.

Overview of Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud

This feature enables configuring a pair of redundant Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) instances in Cisco Catalyst SD-WAN cloud gateways, using the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager. Using redundant routers to form the cloud gateway offers path resiliency to the public cloud. Using the Cisco Catalyst SD-WAN fabric, this feature enables your branch and data center devices to communicate with applications and services in Google Cloud. It also lets you achieve site-to-site connectivity using Google Cloud's global network.

The Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager automates the bring-up of the WAN Virtual Private Cloud (VPC) and two transit VPCs in Google Cloud. The workflow also discovers your existing VPCs in geographical Google Cloud regions. You can then create tags for the discovered VPCs in Cisco SD-WAN Manager. These tags are used to map your service VPNs to specific VPCs in your public cloud infrastructure. This mapping enables the following—connectivity to your workload VPCs in Google Cloud, and site-to-site connectivity using Google Cloud's global network.

Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway

Minimum release: Cisco vManage Release 20.9.1

You can deploy a minimum of two and a maximum of eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region. By adding more than two instances, that is, horizontally scaling up the number of instances, you can increase the throughput. You can horizontally scale the number of instances between the minimum limit of two and the maximum limit of eight instances based on the required throughput.

When you deploy a cloud gateway with only two Cisco Catalyst 8000V instances, each instance is deployed in a different zone of the region to provide redundancy. When you deploy a cloud gateway with more than two instances, the instances are deployed in two or more zones for redundancy. The instances may not be evenly distributed among the zones.

Note Ensure that all the Cisco Catalyst 8000V instances that are part of a cloud gateway are of the same instance type.

Related Topics

Create and Manage Cloud Gateways, on page 392

Google Service Directory Integration and Lookup

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Google Service Directory is integrated with Cisco Catalyst SD-WAN. Google Service Directory is a catalog of your applications or services in Google Cloud. When you enable Service Directory Lookup in Cisco SD-WAN Manager, this integration allows Cisco SD-WAN Manager to discover your applications that are hosted in Google Cloud, and display them as Cloud Discovered applications. You can then use such applications to define application-aware routing policies.

For information on creating a Google Service Directory, and registering new services in your Google Service Directory, see Google documentation.

How Google Service Directory Lookup Works

1. Google Service Directory lookup is configured from the **Cloud Global Settings** and **Associate Cloud Account** windows in the **Cloud OnRamp for Multicloud** workflow in Cisco SD-WAN Manager.

   For accounts configured as Service Directory Lookup Capable, lookup results are displayed every 20 minutes in the Cisco SD-WAN Manager task bar.

2. Cisco SD-WAN Manager discovers applications in your Google Service Directory by looking up the Google regions associated with the account.

3. Cisco SD-WAN Manager finds the namespaces in the Google region associated with the account, followed by a list of services or applications in each of the namespaces.

4. Cisco SD-WAN Manager fetches the endpoint list and metadata for each service discovered under the namespace. The metadata or service annotation includes attributes such as the traffic profile.

   Cisco SD-WAN Manager looks for the keyword *trafficProfile* key in the list of annotations of the service. Next, it checks if the value against this key is one of the known SLA keywords—data, voice, video, critical, realtime, best-effort, or default. If the value does not match, the traffic profile for the service is set as default. If the keyword *trafficProfile* is not found, the traffic profile is set to default. The traffic profile of the service is automatically translated into an appropriate SLA class, which can be used while creating centralized policies.

   As part of the lookup, Cisco SD-WAN Manager verifies the endpoint list against your current Google Cloud mapping state. This determines whether the service is reachable through Cisco SD-WAN Manager.

5. Each discovered service that is reachable through Cisco SD-WAN Manager is cataloged as a Cloud Discovered application.

   The name of the cloud-discovered application is derived by concatenating the following: Google account name, region name, the name of the namespace, and the name of the service or application in Google cloud. The subfields of the names are joined together with a hyphen. The length of the cloud-discovered application name is subject to a limit of 59 characters. Cisco SD-AVC may have issues in adding the

application if the name exceeds this character limit. This can result in the application not being used correctly in policies.

Therefore, while deciding the name of the application in Google Cloud, we recommend that you consider the logic used for determining the name of the cloud-discovered application in Cisco SD-WAN Manager.

Note If a previously discovered service or application is no longer available in Google Cloud, Cisco SD-WAN Manager removes that application. If such an application is used in a policy, an alarm is generated and you need to remove the application from the policy manually. The packets meant for the removed service could still reach the cloud, but may be dropped after they reach the cloud.

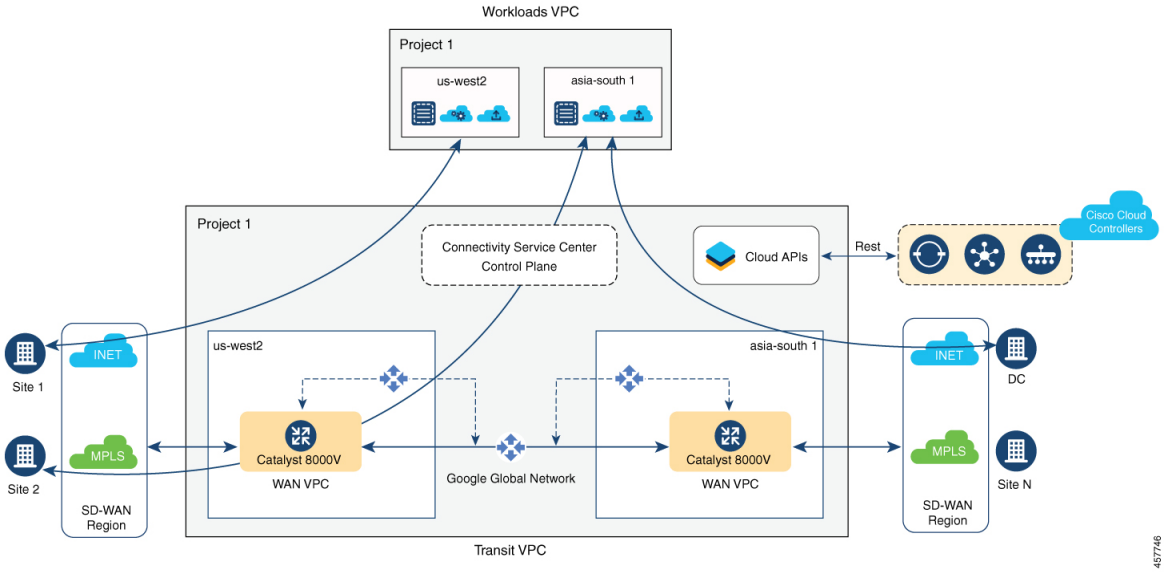
Connectivity Models

The Cisco Catalyst SD-WAN cloud gateway with Google Cloud feature supports the following connectivity models:

Site to Google Cloud

This use case is applicable when a branch site needs to access an application running in a VPC in Google Cloud. In this scenario, a branch site connects to the WAN VPC, which connects to the workload or applications VPC, through the site to cloud transit VPC.

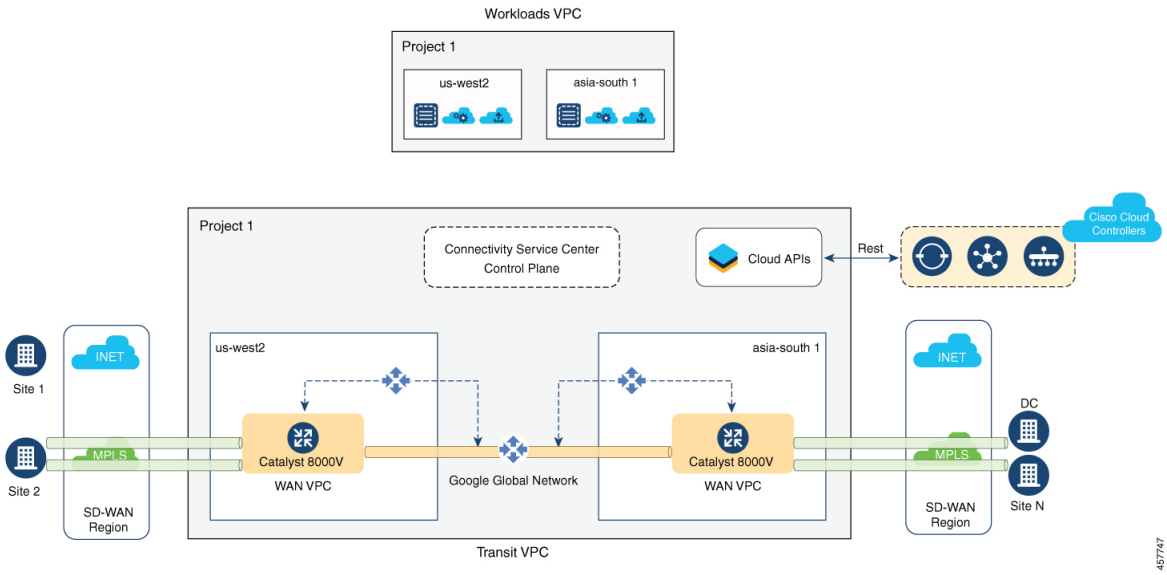
Figure 23: Site to Cloud Connectivity



Site to Site

This use case is applicable for connecting two branches, in different regions, through site-to-site transit VPC using Google Cloud's global network. While it's also possible to connect branches through the public internet, connecting them through Google Cloud's global network ensures optimized transit.

Figure 24: Site to Site Connectivity



Note Site-to-site connectivity can't be enabled between specific cloud gateways or Google Cloud regions. It can be enabled only globally, between all your cloud gateways.

From Cisco vManage Release 20.9.1, after you enable site-to-site connectivity globally for all your cloud gateways, you can configure some cloud gateways so that they don't participate in site-to-site communication (see Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways, on page 386).

Note For the site-to-site connectivity use case, you can define a control policy for intelligent steering of traffic based on your requirement. For example, you may want to use the public internet and Google Cloud's global network for exchanging non-critical and critical traffic flows respectively. For more information, see Centralized Policies.

Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways

Minimum release: Cisco vManage Release 20.9.1

Cisco vManage Release 20.8.1 and earlier releases: you enable or disable site-to-site connectivity for all the cloud gateways in your deployment using the global settings field **Site-to-site Communication**.

- If you disable site-to-site connectivity in the global settings, you can create cloud gateways only in regions that support site-to-cloud connectivity. These cloud gateways can participate in only site-to-cloud communication.

- If you enable site-to-site connectivity in the global settings, you can create cloud gateways only in regions that support site-to-site connectivity. These cloud gateways can participate in both site-to-site and site-to-cloud communication. However, fewer regions support site-to-site connectivity than regions that support only site-to-cloud connectivity. As a result, you have fewer options to take advantage of site-to-cloud connectivity.

From Cisco vManage 20.9.1: You enable or disable site-to-site connectivity for all the cloud gateways in your deployment using the global settings field **Site-to-site Communication**.

- If you enable site-to-site connectivity in the global settings, while creating a cloud gateway, you can choose whether the cloud gateway will participate in site-to-site communication or not, using the field **Involved in Site-to-site communication**.
  - If you decide that a cloud gateway will not participate in site-to-site communication, you can create the gateway in any region that supports only site-to-cloud connectivity.
  - If you decide that a cloud gateway will participate in site-to-site communication, you can create the gateway in any region that supports site-to-site connectivity. The cloud gateway can participate in both site-to-site and site-to-cloud communication in the supported region.

  As a result, you can create some cloud gateways that participate in site-to-site and site-to-cloud communication, and some that participate in only site-to-cloud communication.
- If you disable site-to-site connectivity in the global settings, you can create cloud gateways only in regions that support site-to-cloud connectivity. You cannot enable site-to-site connectivity for a particular cloud gateway if this type of connectivity is disabled globally.

Related Topics

Configure Cloud Global Settings, on page 390
Create and Manage Cloud Gateways, on page 392

Configure Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud

This section describes how to configure the Cisco Catalyst SD-WAN cloud gateways with Google Cloud feature using Cisco SD-WAN Manager. The section also lists the prerequisites that should be met to be able to configure the feature.

Configuration Prerequisites

- You should have a subscription to Google Cloud. You need your Google Cloud account details to associate your account with Cisco SD-WAN Manager.
- To be able to register you Google Cloud service account in Cisco SD-WAN Manager, ensure that you have at least the following roles configured for your Google Cloud account:
  - Service Account User
  - Compute Instance Admin (v1)
  - Compute Network Admin

- Compute Public IP Admin
- Compute Security Admin
- Hub & Spoke Admin
- Spoke Admin

- Ensure that following Google Cloud APIs are enabled in the relevant project:
  - Compute API,
  - Billing API,
  - Network Connectivity Center Alpha API
- Ensure that Cisco SD-WAN Manager is connected to the internet and is able to communicate with Google Cloud to authenticate your account.
- Ensure that Cisco SD-WAN Manager has two Cisco Catalyst 8000V instances that are free to use for creating the WAN VPC. For throughput requirements that exceed 250 Mbps, Cisco Catalyst 8000V license is required.
- Ensure that all Cisco SD-WAN Control Components (Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator) run Cisco SD-WAN Release 20.5.1 or later, and that Cisco Catalyst 8000V instances run Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later.
- Ensure that two Cisco Catalyst 8000V instances are attached to the device template. For more information, see Attach Device to a Device Template.

Note Ensure that you attach the Cisco Catalyst 8000V to the factory default template for Google Cloud (Default_GCP_C8000V_Template_V01).

- Ensure that Cisco Catalyst SD-WAN TCP and UDP ports are open. For more information, see Firewall Ports for Cisco SD-WAN Deployments.

Attach Cisco Catalyst 8000V Instances to a Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

3. From the **Template Type** drop-down list, choose **Default**.

   A list of default templates is displayed.
4. Choose the factory default template for Google Cloud (Default_GCP C8000V_Template_V01).

5. Attach two Cisco Catalyst 8000V instances that are free to use, to the device template. For more information, see Attach Device to a Device Template.

Note After you attach the instances, you should not specify **private1** as the color of the transport location (TLOC) because **private1** is used only for site-to-site communication.

Associate Your Google Cloud Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Setup**, click **Associate Cloud Account**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. Enter the requested information:

Field	Description
Cloud Account Name	Enter a name for your Google Cloud account.
Description (optional)	Enter a description for the account.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.
Billing ID	(Optional) Enter the billing ID associated with your Google Cloud service account. **Note** Enter the billing ID only after the initial account association. If you provide a billing ID, it goes through an automatic validation process. **Note** This field is visible only if you choose the **Yes** option for the **Use for Cloud Gateway** field.
Service Directory Lookup **Note** This field is available in Cisco vManage Release 20.6.1 and later only.	Choose **Enabled** to allow Cisco SD-WAN Manager to discover services or applications in the Google Service Directory associated with the Cloud Account. The option **Disabled** is chosen by default.

Field	Description
Private Key ID	Click **Upload Credential File**. You must generate this file by logging in to Google Cloud console. The private key ID may be in JSON or REST API formats. The format depends on the method of key generation. For more details, see Google Cloud documentation. **Note** Ensure that the JSON file downloaded from Google Cloud does not have an entry with the name of **universe_domain**.

5. Click **Add**.

Configure Cloud Global Settings

Cloud global settings for a cloud provider apply to cloud gateways for the provider, unless you customize the settings on the **Create Cloud Gateway** page.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.

Note The **Enable Configuration Group** option is reserved for future use.

2. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
3. To add global settings, click **Add**. If the cloud global settings are already configured, click **Edit** to modify them.
4. In the **Software Image** field, choose the software image of the WAN edge device for the WAN VPC. This should be a preinstalled Cisco Catalyst 8000V instance.
5. In the **Instance Size** field, from the drop-down list, choose an instance based on your requirements.
6. In the **IP Subnet Pool** field, specify the IP subnet pool for the SD-WAN cloud gateway in Google Cloud. This subnet pool needs prefixes between /16 and /21.
7. In the **Cloud Gateway BGP ASN Offset** field, specify the autonomous system number (ASN) for the cloud gateway for BGP peering. This is the starting offset for the allocation of ASNs for the cloud gateways and Google Cloud routers. Starting from the offset, 10 ASN values are reserved for allocating to the cloud gateways.

Attention This offset value cannot be modified after a cloud gateway is created.

8. For **Intra Tag Communication**, choose **Enabled**. This ensures that VPCs with the same tag can communicate with each other.

9. For **Site-to-Site Communication**, choose **Enabled** for site-to-site transit connectivity using the Google global network. Otherwise, choose **Disabled**.
10. In the **Site-to-Site Tunnel Encapsulation Type** field, choose the encapsulation from the drop-down list.
11. For **Service Directory Lookup Capable**, choose **Enabled** to allow Cisco SD-WAN Manager to discover Google Service Directory applications associated with this Google account. **Disabled** is chosen by default.



Note This field is available for Cisco vManage Release 20.6.1 and later only.

12. In the **Service Directory Poll Timer Value** field, the value is set to 20 minutes by default.

    This field is available for Cisco vManage Release 20.6.1 and later only.
13. In the **Network Service Tier** field, choose one of the Google Cloud service tiers.
    - PREMIUM: Provides high-performing network experience using Google global network.
    - STANDARD: Allows control over network costs.
14. Click **Save** or **Update**.

Discover Host VPCs and Create Tags

After you associate your Google Cloud account with Cisco SD-WAN Manager, you can discover your host VPCs in the regions associated with your Google Cloud account. This workflow shows your cloud infrastructure at a VPC level. You can create new tags for the discovered VPCs, or modify or delete existing tags. Tags are used to manage connectivity between the VPCs and Cisco Catalyst SD-WAN branch VPNs.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Discover** workflow, click **Host Private Networks**.
3. In the **Cloud Provider** field, choose **Google Cloud**.

   A list of discovered host VPCs displays in a table with the following columns: Cloud Region, Account Name, Host VPC Name, Host VPC Tag, Account ID, and Host VPC ID.
4. Click the **Tag Actions** drop-down list to do any of the following:
   - **Add Tag:** Create a tag for a VPC or a group of VPCs.
   - **Edit Tag:** Change the selected VPCs for an existing tag.
   - **Delete Tag:** Delete the tag for the selected VPC.

Create and Manage Cloud Gateways

When the first cloud gateway is created, three reserved VPCs are instantiated—WAN transit VPC, site-to-site transit VPC, and site-to-cloud transit VPC. Cisco Catalyst 8000V instances that are instantiated as part of the cloud gateway are anchored to the VPCs.

This procedure describes how to create a Cisco Catalyst SD-WAN cloud gateway with Google Cloud.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Manage**, click **Create Cloud Gateway**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. In the **Cloud Gateway Name** field, enter a name for your cloud gateway.

Note Ensure that the name is in lowercase letters. See the Google Cloud documentation for information about Naming resources and Naming convention.

5. (Optional) Enter a **Description**.
6. In the **Account Name** field, chose your Google Cloud account name from the drop-down list.
7. In the **Region** field, choose a Google region from the drop-down list.
8. (Minimum release: Cisco vManage Release 20.9.1) **Involved in Site-to-site communication**: If the cloud gateway will participate in site-to-site communication, click **Yes**. If the cloud gateway will not participate in site-to-site communication, click **No**.

Note This field is enabled for configuration only when **Site-to-site Communication** is enabled in the global settings. When **Site-to-site Communication** is disabled in the global settings, this field is dimmed.

9. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
10. (Optional) In the **Settings** section, enter the requested information.

Note You can use either the cloud global settings or customize settings for individual cloud gateways using the fields below.

   a. In the **Software Image** field, choose the software image of the WAN edge device to be instantiated in the WAN VPC to connect your site to Google Cloud.
   b. In the **Instance Size** field, choose an instance size for Cisco Catalyst 8000V, based on your requirements.
   c. In the **IP Subnet Pool** field, specify the IP subnet pool to be used for the Google Cloud WAN VPC. This subnet pool needs prefixes between /16 and /21.

Note The IP subnet pool must not overlap with the IP subnet pool specified in Cloud Global Settings.

d. In the **Network Service Tier** field, choose one of the Google Cloud network service tiers from the drop-down list.

- PREMIUM: Provides high-performing network experience using Google Cloud global network.
- STANDARD: Allows control over network costs.

11. UUID (specify 2):

Cisco vManage Release 20.8.1 and earlier: Choose two Cisco Catalyst 8000V licenses from the drop-down list.

Cisco vManage Release 20.9.1 and later: Choose a minimum of two and a maximum of eight Cisco Catalyst 8000V licenses from the drop-down list.

Note

- All the Cisco Catalyst 8000v instances in a cloud gateway must be of the same instance type. Vertical scaling is not supported.
- From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

Choose the UUIDs that you attached to the default Google Cloud template.

12. (Minimum release: Cisco vManage Release 20.10.1) In the **Multi-Region Fabric Settings** area, for **MRF Role**, choose **Border** or **Edge**.

This option is available only when Multi-Region Fabric is enabled.

13. Click **Add**.

Map VPC Tags and Branch Network VPNs

To enable VPC to VPN mapping, discover a set of VPCs in one or multiple Google regions and create a tag. Then select the service VPNs that you want to map the VPCs to using the same tags.

How Mapping and Connectivity Work

- You don't have to explicitly create connectivity. Based on VPC tags, connectivity is automatically established when cloud gateways are instantiated in a certain region or when tagging operations take place.
- Connectivity intent for inter-tag and intra-tag mapping can be defined independent of the presence of cloud gateways in various cloud regions. The intent is preserved and mapping is realized when a new cloud gateway or mapping change is discovered.
- When cloud gateways are instantiated in different regions, the mapping intents in those regions are automatically realized.

- Inter-tag and intra-tag mapping is based on VPC peering and automatically enables bidirectional connectivity only.
- Only one service VPN can be mapped to one or more tags.
- You can perform only a single cloud operation, such as, tagging, mapping, or, creation or deletion of a cloud gateway, at a time. When one operation is being performed, the others are locked.
- All cloud operations are time bound. For example, mapping operations time out after 60 minutes. On timeout, the operations are declared as failed. Timeout values cannot be configured.
- The Intent Management page doesn't autorefresh when a new mapping intent is being realized.

Prerequisites for Successful Mapping

- VPCs that are involved in mapping (as part of tags) require at least one subnet.
- Mapping relies on VPC peering. Subnets in peering VPCs must be compliant with RFC1918.
- VPCs cannot have overlapping classless interdomain routing (CIDR) addresses. Overlapping CIDR addresses leads to mapping failure.

View or Edit Connectivity

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Intent Management**, click **Cloud Connectivity**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.

   The window displays a connectivity matrix showing source VPNs, and their destinations. The following legend provides information about the status of the intent:

   - Blue: Intent Defined
   - Green: Intent Realized
   - Red: Intent Realized With Errors

   Click any of the cells in the matrix to get a more detailed status information.
4. To define or record a new intent, click **Edit**.
5. Choose the cells that correspond to a VPN and the VPC tags associated with it, and click **Save**.

Service Directory Lookup and Traffic Policies with Discovered Apps

To use services or applications from your Google Cloud account in Cisco SD-WAN Manager traffic policies, you need to first enable Service Directory Lookup in Cisco SD-WAN Manager, and then use the applications discovered from this lookup to create traffic policies.

Enable Service Directory Lookup

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Google Service Directory has been integrated with the Cisco Catalyst SD-WAN solution. With this integration, Cisco SD-WAN Manager can perform a lookup of the Google Service Directories that are part of your Google Cloud Account that is associated with Cisco SD-WAN Manager. Cisco SD-WAN Manager displays the applications or services in your Service Directory as custom applications, which can be used to define routing policies.

For Cisco SD-WAN Manager to be able to search through your Google Service Directory, you need to enable Service Directory Lookup in Cisco SD-WAN Manager.

Naming of Cloud-Discovered Custom Applications

Service Directory Lookup queries Google Cloud for services that you have defined in Google Cloud. Cisco SD-WAN Manager automatically creates custom applications in Cisco Catalyst SD-WAN for the services. To create the name of the custom application, Cisco SD-WAN Manager uses a combination of the following fields, as defined in Google Cloud: Google Cloud account name, Google Cloud region name, service name and namespace. The maximum length for the cloud-discovered custom application name is 59 characters, due to a limitation of the SD-AVC component.

You can view the application list page, showing the custom applications in Cisco SD-WAN Manager. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**, then click **Custom Options** and choose **Lists**. To view the custom applications that Cisco SD-WAN Manager has generated from the services discovered by Cloud OnRamp for Multicloud, click **Cloud Discovered**.

- Cisco SD-WAN Manager 20.6.x handles the 59-character limit as follows: When Cisco SD-WAN Manager uses the four fields described above to create a name for a custom application, if the name exceeds 59 characters, it truncates the name. Truncating the name may lead to name collisions.

  The account name and region name lengths are variable, so it is difficult to predict how many characters remain available for the service name and namespace, while remaining within the 59-character limit.

  To avoid exceeding the character limit, we recommend that when you define services in Google Cloud, use short names for service and name space names. The available length of these names depends on the combined length of the Google Cloud account name and Google Cloud region name.

  - The following example has long account and region names, requiring short service and name space names:

    Account name: gcp-organization-sw-dev
    Region name: australia-southeast1
    Service name: serv1
    Namespace name: nspace1

  - The following example has shorter account and region names, enabling longer service name and name space names:

    Account name: cisco
    Region name: us-west
    Service name: service-xyz
    Namespace name: dev-team

- Beginning with Cisco SD-WAN Manager 20.7.x, you can use longer, more meaningful names for the namespace and service name fields for a service defined in Google Cloud. If necessary, to meet the 59-character maximum, Cisco SD-WAN Manager may truncate part of the service name.

Cisco SD-WAN Manager applies a limit of 12 characters for the Google Cloud account name, a limit of 23 characters for the Google Cloud region name, and a limit of 8 characters for the namespace. Three (3) characters are used for a separator (-) in the custom application name. To remain within the 59-character limit without a truncated service name, use a maximum of 13 characters when providing a service name for a service in Google Cloud. If you use a longer name and the combination of these fields exceeds 59 characters, Cisco SD-WAN Manager truncates the name. If truncating the name causes a name collision with a previously defined custom application, Cisco SD-WAN Manager displays an alarm on the application list page. (Instructions for opening the application list page appear above.)

Before You Begin

Ensure that SD-AVC is enabled in Cisco SD-WAN Manager.

- Enable SD-AVC in Cisco SD-WAN Manager:
  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
  2. For the desired Cisco SD-WAN Manager instance, click **...**, choose **Edit**, and check the **Enable SD-AVC** check box.
- Ensure that Service Directory APIs are enabled for your Google Cloud account.

Enable Service Directory Lookup

1. Enable Service Directory Lookup from the **Associate Cloud Account** window in the **Cloud OnRamp for Multicloud** workflow.

   For more information, see the *Associate Your Google Cloud Account with Cisco SD-WAN Manager* topic in this chapter.
2. Under **Cloud Global Settings** enable the Google Account associated with Cisco SD-WAN Manager as **Service Directory Lookup Capable**, and configure the **Service Directory Poll Timer Value**.

   For more information, see Configure Cloud Global Settings.

Create Traffic Policies Using Cloud Discovered Apps

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Under **Centralized Policy**, click **Lists**.

   You are redirected to the **Application** section under **Policies**.
4. Click **Cloud Discovered**.

   A list of applications discovered from Google Service Directory Lookup is displayed.
5. Click **Map Traffic Profiles**. In the dialog box that appears, you can set or modify the traffic profiles for the discovered service.
6. For each of the traffic profiles, click **vManage SLA Classes** and choose an SLA class to map the application to.
7. Click **Save**.

8. Next, create an application list to include the cloud discovered applications. For more information, see Configure Application List.
9. To create a traffic policy using the discovered applications, click **Custom Options** > **Traffic Policy**, and then click **Add Policy**.

   To configure traffic rules on the application list for the cloud discovered applications, see Configure Traffic Rules in Application-Aware Routing.

Monitor Connectivity

When you create a new cloud gateway, you can verify the bring-up and reachability of the Cisco Catalyst 8000V instances provisioned inside the cloud gateway.

Option 1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Cloud**, the **Network Snapshot** displays a summary of the cloud gateways, host VPCs, and WAN edge devices for various cloud providers.

   The upward arrow next to the WAN edge devices indicates the number of devices that are up. Click the arrow to view additional details of the devices.

Option 2

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Workflows** section, click **Cloud Connectivity** under **Intent Management**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. Click any cell on the page to view the connectivity status of VPNs and VPC tags.

Audit

Starting from Cisco vManage Release 20.6.1, the **Audit** option in the **Cloud OnRamp for Multicloud** workflow is enabled for Google Cloud. Use this option to verify whether the Google Cloud state is in sync with Cisco SD-WAN Manager state. As part of the audit, if the cloud state is identified as out of sync with Cisco SD-WAN Manager state, Cisco SD-WAN Manager automatically tries to resolve the issues and bring parity in the states.

As part of the audit mechanism, the existence of cloud objects, their interrelationships, and their states are all verified against the connectivity intent defined in Cisco SD-WAN Manager. Cisco SD-WAN Manager then takes corrective action is taken if a mismatch is identified.

The following table provides details about the audit discrepancies and fixability for Google Cloud:

Table 73: Examples of GCP audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message
Missing Network Connectivity Center (NCC) spokes	**Report Type**: NCC_HUB **Details**: Spoke <spoke-name> in region <region-id> is missing.
Missing NCC Hubs	**Report Type:** NCC_HUB **Details:** NCC Hub: <Hub Name> not found.
Missing Google cloud routers (GCRs) - primary, secondary, or both	**Report Type:** GCR **Details**: <GCR Name> not found.
Missing site-to-cloud peering of VPCs mapped to VPNs in Cisco SD-WAN Manager	**Report Type**: MAPPING **Details**: Connectivity element was missing from response: [srcType:VPN dstType:VPC dst:<dst-vpc-id>]
Missing VPC peering of VPCs that are mapped to other VPCs in Cisco SD-WAN Manager	**Report Type:** MAPPING **Details:** Connectivity element was missing from response: [srcType:VP dstType:VPC dst:<dst-vpc-id>]
Missing custom routes	**Report Type:** Mapping **Details:** Connectivity element was missing from response: [srcType:VPI src:<C8Kv-Device-UUID>::<vpn-id> dstType:VPC dst:<vpc-id>]
Missing Border Gateway protocol (BGP) sessions	**Report Type**: MAPPING **Details**: BGP session is missing in GCR
Stale BGP sessions	**Report Type**: MAPPING **Details**: Stale prefixes found in BGP Sessions
Removal of a cloud gateway or any of its components	**Report Type:** CGW_ROUTER **Details:** CGW Router: [<CGW Instance name> <region-id>] Couldn't fi cloud (Irrecoverable error, user intervention needed to fix things in cloud
Issues with host VPCs with overlapping CIDRs	**Mapping Failure**: Additional details: Overlapping subnets part of mappi Mapping: VPN:<vpn id> --> <s2c vpc name, vpc-id, vpc-subnet> / <vpc na **Report Type**: Mapping **Details**: vpnAttachSpec with tunnelId: <c8kv uuid>::<vpn id> was miss
Issues with site-to-site VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2S_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).
Issues with site-to-cloud VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2C_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).

Anomaly / Trigger	Audit Findings / Error Message
Issues with WAN VPCs	**Report Type:** TVPC **Details:**TVPC: [<s2c-vpc-id> WAN_VPC] not found in cloud (Irrecove needed to fix things in cloud).
Invalid GCP Credentials	**Report Type:** Account **Details:** Invalid GCP Credentials found for account Id <acc-id>

Note Audit-fix performs the same steps in both on-demand fix (that is, clicking the **Fix Sync Issues** button) and periodic audit followed by auto-correct.

View Cloud Resource Inventory

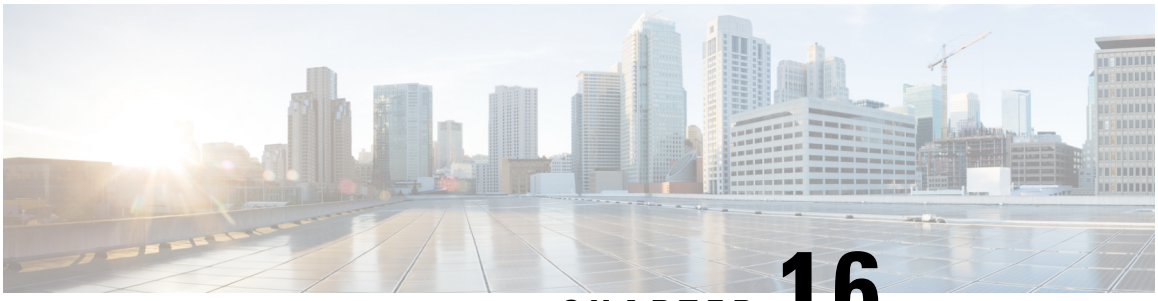
Starting from Cisco vManage Release 20.6.1, you can use the **Cloud Resource Inventory** option in Cisco SD-WAN Manager is enabled for Google Cloud. Use this option to view details of the cloud objects and their identifiers for the Google Cloud account associated with Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu. choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Manage**, click **Gateway Management**.

   Your existing cloud gateways are displayed.
3. For the desired cloud gateway, click **…** and choose **Cloud Resource Inventory**.

The Cloud Resource Inventory options retrieves the following information for the selected cloud gateway:

- VPCs: WAN, site-to-site, and site-to-cloud VPCs.
- VPC Subnets: WAN, site-to-site, and site-to-cloud in each Google Cloud region associated with the Google Cloud account.
- VMs: A pair of Cisco Catalyst 8000V instances in each Google Cloud region.
- Google Cloud Routers: A pair each of site-to-cloud and site-to-site Google Cloud routers in each region.
- Hubs: An instance each of site-to-site and site-to-cloud Google Global Network hubs.
- Spokes: A pair of spokes from each region that is connected to the site-to-site and site-to-cloud hub.



CHAPTER 16

Cisco Catalyst SD-WAN Manager Support for Monitoring Multicloud Services

Table 74: Feature History Table

Feature Name	Release Information	Release Information
Cisco SD-WAN Manager Support for Monitoring Multicloud Services	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to monitor your multicloud network using the Cisco SD-WAN Manager UI.
Monitoring MultiCloud Services for Real Time Data in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature provides enhancements to monitoring dashboard for all the Cloud and Interconnect connections. This feature also gives you the flexibility to specify which dashlets to view and sort them based on your preferences.

- Restrictions for Monitoring Multicloud Services using Cisco SD-WAN Manager , on page 401
- Information about Monitoring Multicloud Services using Cisco SD-WAN Manager, on page 402
- Geographical View, on page 402
- Cloud and Interconnect Dashboard, on page 403
- Cloud Gateway Summary View, on page 404
- Interconnect Gateway Summary View, on page 404

Restrictions for Monitoring Multicloud Services using Cisco SD-WAN Manager

- The feature supports the multi-tenant mode of operation from Cisco vManage Release 20.7.1. With Cisco vManage Release 20.6.x, this feature does not support the multi-tenant mode of operation.
- The feature supports the Interconnect Type Equinix from Cisco vManage Release 20.7.1. With Cisco vManage Release 20.6.x, this feature does not support the Interconnect Type Equinix.
- Geographical locations and traffic statistics are not available when the solution is branch connect-AWS.

Information about Monitoring Multicloud Services using Cisco SD-WAN Manager

This feature enables you to monitor Cisco SD-WAN connectivity to different cloud resources using Cisco SD-WAN Manager. This feature introduces the following views in the UI using which you can visually monitor the approximate geographical locations of Edge devices, cloud types, and information about cloud sites and accounts for different cloud providers:

- Geographical View
- Cloud and Interconnect Dashboard
- Cloud Gateway Summary View
- Interconnect Gateway Summary View

By default, the **Monitor Overview** dashboard displays all the available dashlets that help you monitor the different components and services of a Cisco SD-WAN overlay network. The customizable dashboard feature enables you to do the following:

- Add dashlets
- Delete dashlets
- Rearrange dashlets
- Restore default settings



Note Starting from Cisco vManage Release 20.10.1, the Multicloud dashlets on the **Monitor Overview** dashboard are displayed as soon as the Cloud or Interconnect provider accounts are associated with Cisco SD-WAN Manager.

Geographical View

The geographical view shows the approximate geographic locations of the Cisco Catalyst 8000V instances in multicloud deployments. The approximate locations are based on the publicly available information from the cloud and interconnect types. The locations are provided for the Google Cloud, AWS, and Azure cloud platforms as well as software-defined cloud interconnects.

To view the geographical locations of multicloud Cisco Catalyst 8000V instances:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. On the map, click a Cisco Catalyst 8000V instance to see the cloud or interconnect type, site-id, and system-ip of that instance.

Cloud and Interconnect Dashboard

The cloud and interconnect dashboard displays a separate panel for each cloud instance and software-defined cloud interconnect. A pie chart shows the sites that are connected to the cloud or the software-defined cloud interconnect and their reachability. The sites are Cisco Catalyst SD-WAN devices of a particular site-id that have a BFD session to the cloud or interconnect Cisco Catalyst 8000V. Each cloud or interconnect panel also displays the following information:

- Number of Cisco Catalyst SD-WAN edge devices
- Registered multicloud accounts
- Gateways
- Tags
- Host VPCs
- Tunnels
- VPN connections

To view information on the cloud and interconnect dashboard:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Multicloud**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Multicloud**.

2. To view information about the Cisco Catalyst SD-WAN edge devices, click the number of **WAN Edge**s to see information about the Cisco Catalyst SD-WAN edge devices. The window that is displayed shows the health (aggregate of the CPU, memory, and hardware state), BFD status, configuration status, reachability, hostname, system IP, chassis number, cloud or interconnect gateway name, device model and version of the device.

   - From **Monitor** > **Multicloud**, when you click on the non-zero number of Cloud or Interconnect Edge devices, the **Monitor** > **Devices** page opens. The Filter criteria on the left pane of the **Devices** window allows you to choose the fields to be displayed from the available options.
   - To view the cloud or software-defined cloud interconnect gateway name, region, account name, health, and description of the all the gateways that are specific to a cloud type, click on the non-zero number of Cloud or Interconnect **Gateways**.
   - To view the details of Cloud or Interconnect Edge devices, click on the non-zero number of Cloud or Interconnect **Edge**.
   - To view the Connected Sites health, BFD status and site ID, click on the non-zero number of **Connected Sites**.

Cloud Gateway Summary View

Note Geographical locations and traffic statistics are not available when the solution is branch connect-AWS.

The cloud gateway summary view displays the following information:

- Cloud type
- Account name
- Region
- Cloud gateway devices
- Associated branch devices—branch devices that have a BFD session set up with the cloud gateway devices.
- Associated VPCs and vNETs—VPCs and vNETs that are mapped to a VPN that belongs to the same region as the cloud gateway.
- Traffic statistics—tunnel statistics from the cloud gateway devices to the workload VPCs. When a device is selected, you can choose to view the following traffic statistics and also for the time duration listed:
  - Kbps
  - Packets
  - Octets
  - Errors
  - Drops
  - Pps

  If no device is selected, an aggregation of statistics of all the devices in the cloud gateway is displayed.

To go to the cloud gateway summary view:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Choose **Cloud**.
3. In the cloud gateway summary table, click the cloud gateway name for which you want to view the details. You can also view details about the connected sites on this page.

Interconnect Gateway Summary View

The interconnect gateway summary view displays the following information:

- Cisco Catalyst SD-WAN edge device type

- Account name
- Region
- Interconnect gateway devices
- Associated branch devices
- Interconnect connectivity

To go to the interconnect gateway summary view:

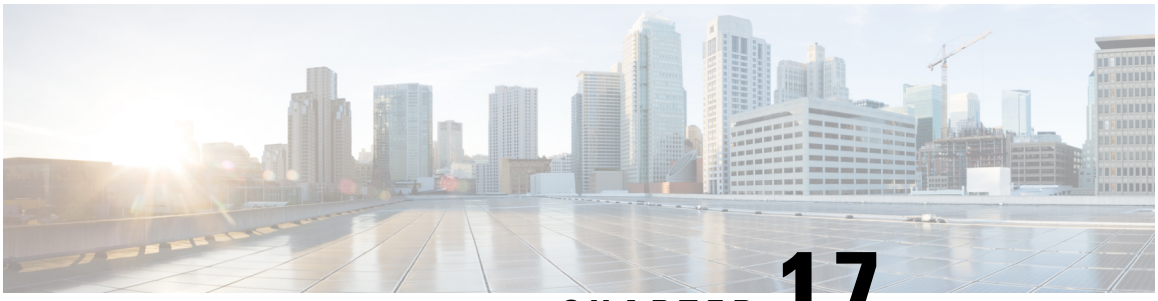
1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Choose **Interconnect**.
3. Click the interconnect gateway name for which you want to view the details.



PART IV

Cloud OnRamp for Multicloud: Cisco Catalyst SD-WAN Cloud Interconnect (Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Earlier)

- Cloud OnRamp for Multicloud: Cisco Catalyst SD-WAN Cloud Interconnect, on page 409
- License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 411
- Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 425
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 497

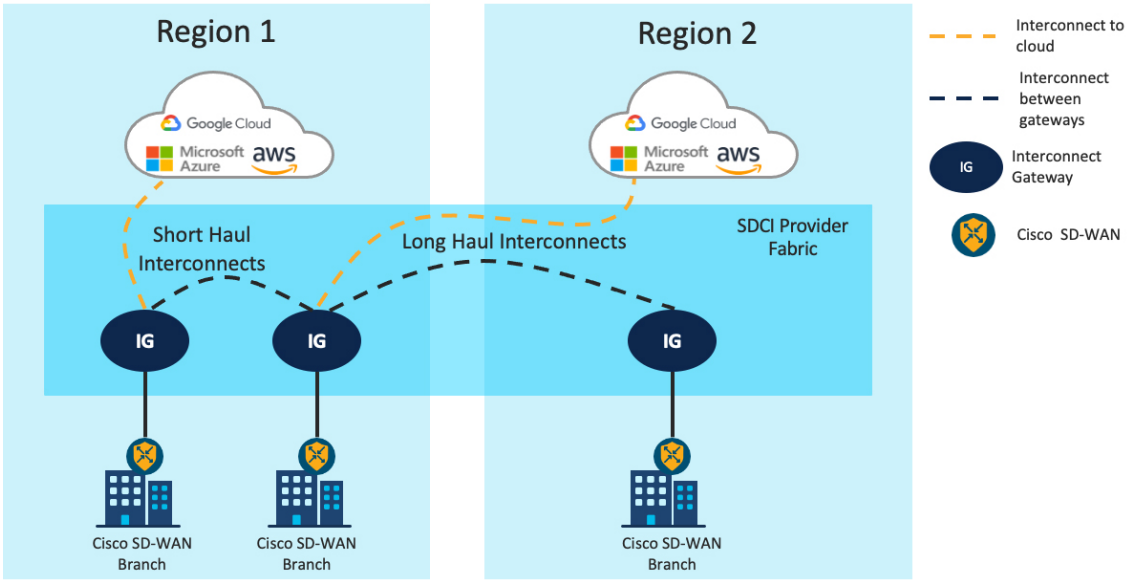


CHAPTER 17

Cloud OnRamp for Multicloud: Cisco Catalyst SD-WAN Cloud Interconnect

From Cisco IOS XE Release 17.5 and Cisco vManage Release 20.5, you can instantiate a Cisco Catalyst SD-WAN edge device within the fabric of a Software-Defined Cloud Interconnect (SDCI) provider and connect a branch location to this edge device through the SD-WAN fabric. From this edge device, you can create software-defined interconnects to other Cisco Catalyst SD-WAN edge devices in the SDCI provider fabric, or to public or private clouds. Thus, the edge devices in the SDCI provider fabric serve as Interconnect Gateways.

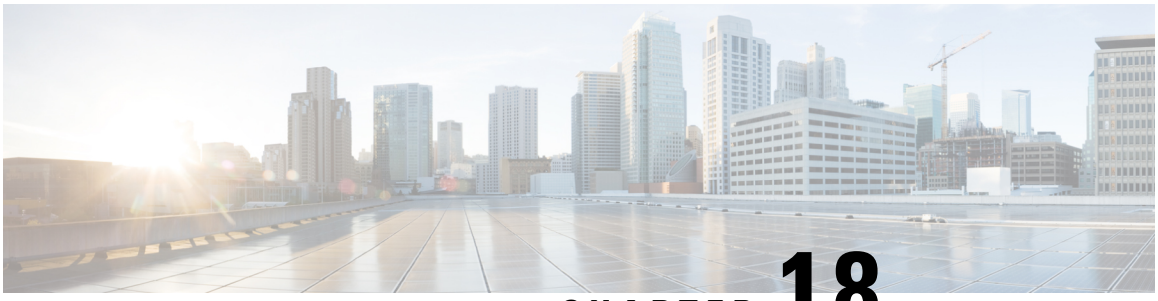
Figure 25: Cisco Catalyst SD-WAN Cloud Interconnects to link SD-WAN branches and SD-WAN branches to Cloud



The software-defined interconnects link branch locations, or link branch locations to cloud service providers. The interconnects provide dedicated private Layer 2 connectivity with SLA-backed assured performance bandwidth and 99.999% availability. Short haul interconnects link branch locations or a branch location and a cloud onRamp in the same region. Long haul interconnects link branch locations in different regions, or a branch location in one region to a cloud onRamp in another region.

Cisco SD-WAN Manager provides a single UI portal through which you can instantiate the edge device in the SDCI fabric and create the software-defined interconnects.

- Cisco SD-WAN Cloud Interconnect with Megaport
- Cisco SD-WAN Cloud Interconnect with Equinix



CHAPTER 18

License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

Table 75: Feature History

Feature Name	Release Information	Description
License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport	Cisco vManage Release 20.9.1	To create Interconnect Gateways and Interconnect Connections in the Megaport fabric, you must purchase required licenses on Cisco Commerce workspace. With this feature, Cisco SD-WAN Manager operates together with Megaport to enable you to monitor your licenses while Cisco and Megaport jointly enforce the license requirements when you create Interconnect Gateways or Interconnect Connections.
Pay-As-You-Go and IP-Transit License Management for Megaport	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature introduces support for the pay-as-you-go (PAYG) license type for Megaport services. The PAYG model is a usage-based model which allows you to pay based on consumption. For example, a cloud storage service provider could charge based on the amount of storage used.

- Information About License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 412
- View Licenses Associated with a Megaport Account, on page 421
- Find License SKU Associated with an Interconnect Gateway, on page 423
- Find License SKU Associated with an Interconnect Connection, on page 423

Information About License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

With the Cisco Catalyst SD-WAN Cloud Interconnect with Megaport solution, Cisco SD-WAN Manager enables you to create site-to-cloud and site-to-site connections that span the Cisco Catalyst SD-WAN overlay and the Megaport fabric. In the site-to-cloud use case, you can connect a Cisco Catalyst SD-WAN branch site to a public cloud service using the Megaport fabric. In the site-to-site use case, you can connect a Cisco Catalyst SD-WAN branch site to another branch site using the Megaport fabric.

The workflow for creating a site-to-cloud connection using Cisco SD-WAN Manager is as follows:

- Deploy a Cisco Catalyst 8000V instance as an Interconnect Gateway at a Megaport Point of Presence (PoP).
- Create an Interconnect Connection in the Megaport fabric between the Interconnect Gateway and the cloud service provider.
- Route traffic from the WAN edge device at the branch to the Interconnect Gateway through the Cisco Catalyst SD-WAN overlay, connecting your branch to the cloud service provider.

The workflow for creating a site-to-site connection using Cisco SD-WAN Manager is as follows:

- Deploy two Cisco Catalyst 8000V instances as Interconnect Gateways at a Megaport Point of Presence (PoP).
- Create an Interconnect Connection in the Megaport fabric between the Interconnect Gateways.
- Route traffic from the WAN edge device at one of the branches to one of the Interconnect Gateways through the Cisco Catalyst SD-WAN overlay.
- Route traffic from the WAN edge device at the other branch to the other Interconnect Gateway through the Cisco Catalyst SD-WAN overlay.

Before you create the Interconnect Gateways and Interconnect Connections in the Megaport fabric, you must purchase the required licenses that are available as Stock Keeping Units (SKUs) on Cisco Commerce workspace. The licenses belong to the following three categories:

- Interconnect Gateway Licenses
- Interconnect Connection Licenses
- Supplemental Licenses

These licenses must be purchased along with the required Cisco Catalyst 8000V licenses and, if necessary, HSEC licenses. If you do not have the required licenses, creation of the Interconnect Gateway or Interconnect Connection fails and Cisco SD-WAN Manager displays an appropriate error message provided by Megaport.

Interconnect Gateway Licenses

An Interconnect Gateway license enables you to deploy an Interconnect Gateway in any metro of a particular region in the Megaport fabric.

While choosing the Interconnect Gateway license, consider the following aspects:

- Deployment region: Deploy the Interconnect Gateway at a Megaport PoP that is nearest to your branch in that region.
- Form factor: Choose a form factor for the Interconnect Gateway based on the maximum cumulative bandwidth of inbound traffic from all the branches that you intend to connect to the gateway.

The SKUs are named in this format: `MVE-<region-code>-<form-factor-code>-C`

- In Megaport terminology, an Interconnect Gateway is referred to as a Megaport Virtual Edge (MVE).
- The region-code identifies a region, which includes one or more metros. In turn, each metro has multiple datacenters for redundancy. The following table lists the available regions, region codes, and the metros within each region.

Region	Region Code	Metros
North America	NA	Ashburn, Atlanta, Bay Area, Chicago, Dallas, Denver, Los Angeles, Miami, New York, Phoenix, Seattle, Toronto
Europe	EU	Amsterdam, Frankfurt, Paris
Asia	ASIA	Hong Kong, Singapore, Osaka, Tokyo
Australia	AU	Melbourne, Perth, Sydney
New Zealand	NZ	Auckland
United Kingdom	UK	London



Note

- The supported metros in a region and supported regions are subject to change based on Megaport expanding to new metros and regions. Check Cisco Commerce Workspace for the up-to-date list of supported metros and regions.
- The availability of a metro for Interconnect Gateway deployment is subject to available compute capacity in the metro.

- The form factor is one of the following:

Form Factor	Form Factor Code	Description
Small	SML	Cisco Catalyst 8000v instance with 2 cores supports a maximum inbound bandwidth of 500 Mbps
Medium	MED	Cisco Catalyst 8000v instance with 4 cores supports a maximum inbound bandwidth of 1 Gbps
Large	LRG	Cisco Catalyst 8000v instance with 8 cores supports a maximum inbound bandwidth of 5 Gbps

- -C at the end of the SKU name indicates that it is a prepaid license.

IP Transit to Interconnect Gateway

Along with the Interconnect Gateway license, you must also purchase a suitable IP transit license on Cisco Commerce Workspace. The IP transit license is for the internet connection at the Megaport PoP. WAN edge devices at the branches connect to the Interconnect Gateway through this internet connection. When you select an Interconnect Gateway license on Cisco Commerce Workspace, the appropriate IP transit license is automatically included for purchase.

The IP transit SKUs are named in this format: `IPT-<region-code>-<form-factor-code>-C`

The region and form-factor codes have the same values as the Interconnect Gateway SKU. -C at the end of the SKU name indicates that it is a prepaid license.

Related Topics

License Enforcement for Interconnect Gateways, on page 417

Interconnect Connection Licenses

You can create two types of Interconnect Connections:

- Within a metro in a Megaport region: The Interconnect Connections within a metro are short-haul connections.
- Between metros: The Interconnect Connections between metros are long-haul connections.

Purchase appropriate licenses for both short-haul and long-haul connections on Cisco Commerce workspace.

Short-Haul Interconnect Connection Licenses

You can create a short-haul Interconnect Connection from an Interconnect Gateway to a cloud onramp instance or to another Interconnect Gateway in the same metro. A short-haul Interconnect Connection acts as a private connect to a cloud service provider within a metro. Short-haul Interconnect Connections have a bandwidth of 1 Gbps or 10 Gbps. Short-haul Interconnect Connections are also referred to as In-Metro (IM) Interconnect Connections.

The short-haul Interconnect Connection SKUs are named in this format:
`VXC-IM-<bandwidth>-<region-code>-C`

- In Megaport terminology, an Interconnect Connection is referred to as a Virtual Cross Connect (VXC). IM denotes In-Metro.
- The region-code identifies a region, which includes one or more metros. In turn, each metro has multiple data centers for redundancy. The following table lists the available regions, region codes, and the metros within each region.

Region	Region Code	Metros
North America	NA	Ashburn, Atlanta, Bay Area, Chicago, Dallas, Denver, Los Angeles, Miami, New York, Phoenix, Seattle, Toronto
Europe	EU	Amsterdam, Frankfurt, Paris
Asia	ASIA	Hong Kong, Singapore, Osaka, Tokyo
Australia	AU	Melbourne, Perth, Sydney
New Zealand	NZ	Auckland

Region	Region Code	Metros
United Kingdom	UK	London

Note The supported metros in a region and supported regions are subject to change based on Megaport expanding to new metros and regions. Check Cisco Commerce workspace for the up-to-date list of supported metros and regions.

A short-haul Interconnect Connection SKU for a region enables you to create an Interconnect Connection in any metro in the region.

- The bandwidth is 1G (representing 1 Gbps) or 10 G (representing 10 Gbps).
- -C at the end of the SKU name indicates that it is a prepaid license.

Long-Haul Interconnect Connection Licenses

You can create a long-haul Interconnect Connection in the following cases:

- From an Interconnect Gateway to a cloud onramp instance in a different metro in the same region or another region. The Interconnect Connection acts as a private connect to a cloud service provider across metros or regions.
- From an Interconnect Gateway to another Interconnect Gateway in a different metro in the same region or another region. The Interconnect Connection connects Interconnect Gateways across metros or regions.

Long-haul Interconnect Connections have one of the following bandwidths: 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, and 10 Gbps.

Long-haul Interconnect Connections are also referred to as Inter/Intra-Region Interconnect Connections.

The long-haul Interconnect Connection SKUs are named in this format:
`VXC-II-<region1-code>-<region2-code>-C`

- In Megaport terminology, an Interconnect Connection is referred to as a Virtual Cross Connect (VXC). II denotes Inter/Intra-Region.
- A region-code identifies a region, which includes one or more metros. In turn, each metro has multiple data centers for redundancy. The following table lists the available regions, region codes, and the metros within each region.

Region	Region Code	Metros
North America	NA	Ashburn, Atlanta, Bay Area, Chicago, Dallas, Denver, Los Angeles, Miami, New York, Phoenix, Seattle, Toronto
Europe	EU	Amsterdam, Frankfurt, Paris
Asia	ASIA	Hong Kong, Singapore, Osaka, Tokyo
Australia	AU	Melbourne, Perth, Sydney

Region	Region Code	Metros
New Zealand	NZ	Auckland
United Kingdom	UK	London

Note The supported metros in a region and supported regions are subject to change based on Megaport expanding to new metros and regions. Check Cisco Commerce workspace for the up-to-date list of supported metros and regions.

A long-haul Interconnect Connection SKU for a region enables you to create an Interconnect Connection in any metro in the region.

- -C at the end of the SKU name indicates that it is a prepaid license.

Related Topics

License Enforcement for Short-Haul Interconnect Connections, on page 418
License Enforcement for Long-Haul Interconnect Connections, on page 419

Supplemental Licenses

To create an AWS hosted connection, in addition to a short-haul or long-haul Interconnect Connection license, you must purchase an AWS hosted connection license on Cisco Commerce Workspace.

To use a long-haul Interconnect Connection as an AWS hosted connection, purchase a SKU that has the format: `AWS-HC-IIVXC-C`

- AWS-HC denotes an AWS hosted connection.
- IIVXC denotes an inter/intra-region VXC or a long-haul Interconnect Connection.
- The permissible bandwidth of the connection is determined by the bandwidth associated with the long-haul Interconnect Connection license.
- -C at the end of the SKU name indicates that it is a prepaid license.

To use a short-haul Interconnect Connection as an AWS hosted connection, purchase a SKU that has the format: `AWS-HC-IMVXC-<bandwidth>-C`

- AWS-HC denotes an AWS hosted connection.
- IMVXC denotes an in-metro VXC or a short-haul Interconnect Connection.
- The bandwidth is 1G (representing 1 Gbps) or 10 G (representing 10 Gbps). The bandwidth of the AWS hosted connection license must match the bandwidth of the short-haul Interconnect Connection license.
- -C at the end of the SKU name indicates that it is a prepaid license.

Related Topics

License Enforcement for AWS Hosted Connections, on page 420

License Enforcement

Cisco and Megaport jointly enforce the entitlements for the licenses purchased through Cisco Commerce workspace.

- When you purchase a license SKU on Cisco Commerce workspace, Megaport is notified of the purchase and the license is added to your Megaport account. You can also view the license information on the **Account Licenses** page Cisco SD-WAN Manager.
- When you create an Interconnect Gateway, an Interconnect Connection, or an AWS hosted connection on Cisco SD-WAN Manager, before creating the resource in the Megaport fabric, Megaport verifies whether you have the necessary licenses.
- If you have the necessary licenses, Megaport changes the license status to in-use and creates the requested resource. The license status is also updated on Cisco SD-WAN Manager.
- If you do not have the necessary licenses, Megaport does not create the requested resource and Cisco SD-WAN Manager displays an error message to indicate that you do not have the necessary licenses. Purchase the necessary licenses on Cisco Commerce workspace and create the resource.
- Cisco SD-WAN Manager raises an alarm 90 days before a license expires. Cisco SD-WAN Manager also raises alarms when a license expires or is renewed on Cisco Commerce workspace.
- Megaport notifies you of license expiration and impending license expiry through emails.

Related Topics

View Licenses Associated with a Megaport Account, on page 421

License Enforcement for Interconnect Gateways

When you create an Interconnect Gateway on Cisco SD-WAN Manager, Cisco SD-WAN Manager sends the request to Megaport. Before approving the request, Megaport checks whether you have the necessary license in your account.

To create the Interconnect Gateway, you must have an Interconnect Gateway license that matches the following criteria:

- The license must not have expired and must not be in use.
- The license must apply to the region in which you wish to create the Interconnect Gateway.
- The license must match the form factor of the Interconnect Gateway you wish to create.
- If you have multiple licenses that are not in use and support the requested region and form factor, the license with the earliest expiration time is selected.

If you have a license that matches the required criteria, Megaport marks the license as being in-use and approves the request to create the Interconnect Gateway.

If you do not have a license that matches the required criteria, Interconnect Gateway creation fails and Cisco SD-WAN Manager displays an appropriate error message such as the following: `No license for <ICGWName> MVE`

Purchase the necessary license on Cisco Commerce workspace or make an in-use license available and try creating the Interconnect Gateway again. When you delete an Interconnect Gateway, the status of the associated license changes to available.

License Expiry

Cisco SD-WAN Manager raises an alarm in the following scenarios:

- 90 days before an Interconnect Gateway license expires
- When an Interconnect Gateway license expires
- When an Interconnect Gateway license is renewed

Upon license expiration, Megaport does not bring down the Interconnect Gateway. Renew the license before expiry or bring down the Interconnect Gateway within 14 days of license expiry. Megaport may charge you directly based on their Global Services Agreement if you do not renew the license within the grace period of 14 days.

Related Topics

Interconnect Gateway Licenses, on page 412

License Enforcement for Short-Haul Interconnect Connections

When you create a short-haul Interconnect Connection on Cisco SD-WAN Manager, Cisco SD-WAN Manager sends the request to Megaport. Before approving the request, Megaport checks whether you have the necessary license in your account.

To create the short-haul Interconnect Connection, you must have a short-haul Interconnect Connection license that matches the following criteria:

- The license must not have expired and must not be in use.
- The license must apply to the region in which the target metro is located.
- The license must match the bandwidth of the Interconnect Connection you wish to create or support a larger bandwidth.
- If you have multiple licenses that are not in use and match the region and the bandwidth, the license with the earliest expiration time is selected.

If a license that matches the bandwidth or a closest license of higher bandwidth meets the required region and availability criteria, Megaport marks the license as being in-use and approves the request to create the short-haul Interconnect Connection.

If you do not have a license that matches the required criteria, short-haul Interconnect Connection creation fails and Cisco SD-WAN Manager displays an appropriate error message such as the following: `Unable to find valid matching license for the Interconnect connection`

Purchase the necessary license on Cisco Commerce workspace or make an in-use license available and try creating the short-haul Interconnect Connection again. When you delete a short-haul Interconnect Connection, the status of the associated license changes to available.

License Expiry

Cisco SD-WAN Manager raises an alarm in the following scenarios:

- 90 days before a short-haul Interconnect Connection license expires
- When a short-haul Interconnect Connection license expires
- When a short-haul Interconnect Connection license is renewed

Upon license expiration, Megaport does not bring down the short-haul Interconnect Connection. Renew the license before expiry or bring down the short-haul Interconnect Connection within 14 days of license expiry. Megaport may charge you directly based on their Global Services Agreement if you do not renew the license within the grace period of 14 days.

Related Topics

Interconnect Connection Licenses, on page 414

License Enforcement for Long-Haul Interconnect Connections

When you create a long-haul Interconnect Connection on Cisco SD-WAN Manager, Cisco SD-WAN Manager sends the request to Megaport. Before approving the request, Megaport checks whether you have the necessary license in your account.

To create the long-haul Interconnect Connection, you must have a long-haul Interconnect Connection license that matches the following criteria:

- The license must not have expired and must not be in use.
- The license must apply to the regions in which the source and target metros are located.



Note The UK does not belong to the EU region. To provision a connection originating or terminating in the UK, ensure that you have an appropriate UK license.

- The license must match the bandwidth of the Interconnect Connection you wish to create or support a larger bandwidth.
- If you have multiple licenses that are not in use and match the regions and the bandwidth, the license with the earliest expiration time is selected.

If a license that matches the bandwidth or a closest license of higher bandwidth meets the required region and availability criteria, Megaport marks the license as being in-use and approves the request to create the long-haul Interconnect Connection.

If you do not have a license that matches the required criteria, long-haul Interconnect Connection creation fails and Cisco SD-WAN Manager displays an appropriate error message such as the following: `Unable to find valid matching license for the Interconnect connection`

Purchase the necessary license on Cisco Commerce workspace or make an in-use license available and try creating the long-haul Interconnect Connection again. When you delete a long-haul Interconnect Connection, the status of the associated license changes to available.

License Expiry

Cisco SD-WAN Manager raises an alarm in the following scenarios:

- 90 days before a long-haul Interconnect Connection license expires
- When a long-haul Interconnect Connection license expires
- When a long-haul Interconnect Connection license is renewed

Upon license expiration, Megaport does not bring down the long-haul Interconnect Connection. Renew the license before expiry or bring down the long-haul Interconnect Connection within 14 days of license expiry.

Megaport may charge you directly based on their Global Services Agreement if you do not renew the license within the grace period of 14 days.

Related Topics

Interconnect Connection Licenses, on page 414

License Enforcement for AWS Hosted Connections

When you create a short-haul or long-haul Interconnect Connection Cisco SD-WAN Manager and intend to use it as an AWS hosted connection, Cisco SD-WAN Manager sends the request to Megaport. Before approving the request, Megaport checks whether you have the necessary short-haul or long-haul Interconnect Connection license, and the supplemental AWS hosted connection license.

- A short-haul Interconnect Connection license must fulfil requirements outlined in the License Enforcement for Short-Haul Interconnect Connections, on page 418 section of this document.
- A long-haul Interconnect Connection license must fulfil requirements outlined in the License Enforcement for Long-Haul Interconnect Connections, on page 419 section of this document.
- The AWS hosted connection license must not have expired and must not be in use.

If an Interconnect Connection license that matches the bandwidth or a closest license of higher bandwidth meets the required region and availability criteria, and the supplemental AWS hosted connection license is available for use, Megaport marks the licenses as being in-use and approves the request to create the long-haul Interconnect Connection.

If you do not have the required licenses, connection creation fails and Cisco SD-WAN Manager displays an appropriate error message such as the following: `Unable to find valid matching license for the Interconnect connection`

Purchase the necessary licenses on Cisco Commerce workspace or make in-use licenses available and try creating the AWS hosted connection again. When you delete an Interconnect Connection being used as an AWS hosted connection, the associated licenses become available to create a new AWS hosted connection.

License Expiry

Cisco SD-WAN Manager raises an alarm in the following scenarios:

- 90 days before the supplemental license expire
- When the supplemental license expires
- When the supplemental license is renewed

Upon license expiration, Megaport does not bring down the AWS hosted connection. Renew the license before expiry or bring down the connection within 14 days of license expiry. Megaport may charge you directly based on their Global Services Agreement if you do not renew the license within the grace period of 14 days.

Related Topics

Supplemental Licenses, on page 416

Information About Pay As You Go License

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1

A PAYG license for Megaport services allows you to pay only for the infrastructure resources that you utilize. The PAYG licensing mechanism requires you to procure PAYG SKUs from Cisco Commerce Workspace (CCW). These PAYG license SKUs bring up any Megaport services without requiring any term commitments. You can dynamically expand or contract your network based on your day-to-day bandwidth requirements and be billed at the end of the month.

For information about creating an interconnect gateway with a PAYG license at a Megaport location, see Create Interconnect Gateway at a Megaport Location.

View Licenses Associated with a Megaport Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. From **SETUP** under **WORKFLOWS**, click **Account Licenses**.
4. **Provider**: From the drop-down list, choose **Megaport**.
5. **Account Name**: From the drop-down list, choose a Megaport account name.
6. To view Interconnect Gateway licenses, click **INTERCONNECT GATEWAY LICENSES**.

   Cisco SD-WAN Manager displays the Interconnect Gateway license SKUs associated with the account, providing the following details for each SKU:

Table 76: Interconnect Gateway License SKU Details

Column	Description
SKU Name	Name of the license SKU
SKU UUID	Unique ID for the license SKU within the Megaport account to which it belongs
Gateway Size	Size or form factor of the Interconnect Gateway instance (SML, MED, or LRG)
State	Current state of the license(IN_USE; IN_USE, EXPIRED; AVAILABLE; or EXPIRED)
License End Date	The end date (expiry date) for the license derived from the start date and the term of entitlement
Start Date	The license start date specified while ordering the SKU on Cisco Commerce workspace
Smart Account ID	Smart Account to which the license belongs
Virtual Account ID	Virtual Account to which the license belongs
Subscription ID	Subscription ID associated with the license
Web Order ID	Unique web order ID for the license

7. To view Interconnect Connection licenses, click **INTERCONNECT CONNECTION LICENSES**.

   Cisco SD-WAN Manager displays the Interconnect Connection license SKUs associated with the account, providing the following details for each SKU:

   Table 77: Interconnect Connection License SKU Details

Column	Description
SKU Name	Name of the license SKU
SKU UUID	Unique ID for the license SKU within the Megaport account to which it belongs
State	Current state of the license(IN_USE; IN_USE, EXPIRED; AVAILABLE; or EXPIRED)
License End Date	The end date (expiry date) for the license derived from the start date and the term of entitlement
Start Date	The license start date specified while ordering the SKU on Cisco Commerce workspace
VXC Bandwidth	Configured bandwidth (in Mbps) of the Interconnect Connection
Smart Account ID	Smart Account to which the license belongs
Virtual Account ID	Virtual Account to which the license belongs
Subscription ID	Subscription ID associated with the license
Web Order ID	Unique web order ID for the license

8. To view supplemental licenses, click **SUPPLEMENTAL LICENSES**.

   Cisco SD-WAN Manager displays the supplemental license SKUs associated with the account, providing the following details for each SKU:

   Table 78: Supplemental License SKU Details

Column	Description
SKU Name	Name of the license SKU
SKU UUID	Unique ID for the license SKU within the Megaport account to which it belongs
State	Current state of the license(IN_USE; IN_USE, EXPIRED; AVAILABLE; or EXPIRED)
License End Date	The end date (expiry date) for the license derived from the start date and the term of entitlement
Start Date	The license start date specified while ordering the SKU on Cisco Commerce workspace

Column	Description
Bandwidth	Configured bandwidth (in Mbps) of the AWS hosted connection
Smart Account ID	Smart Account to which the license belongs
Virtual Account ID	Virtual Account to which the license belongs
Subscription ID	Subscription ID associated with the license
Web Order ID	Unique web order ID for the license

Find License SKU Associated with an Interconnect Gateway

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. From **MANAGE** under **WORKFLOWS**, click **Gateway Management**.

   Cisco SD-WAN Manager displays all the deployed Interconnect Gateways in a table.
4. Find the Interconnect Gateway of interest.

Tip Search for an Interconnect Gateway using the name you specified for it during configuration.

5. Scroll to the right to view the **License SKU UUID** column.

   On the **Account Licenses** page, use this SKU UUID to view more information about the license SKU.

   The **License End Date** column displays the expiry date for the Interconnect Gateway license.

Related Topics

View Licenses Associated with a Megaport Account, on page 421

Find License SKU Associated with an Interconnect Connection

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. From **INTENT MANAGEMENT** under **WORKFLOWS**, click **Interconnect Connectivity**.

   Cisco SD-WAN Manager displays all the configured Interconnect Connections in a table.
4. Find the Interconnect Connection of interest.

Tip Search for the Interconnect Connection using the name you entered for it during configuration.

5. Scroll to the right to view the **Connection License SKU UUID** column. On the **Account Licenses** page, use this SKU UUID to view more information about the license SKU.

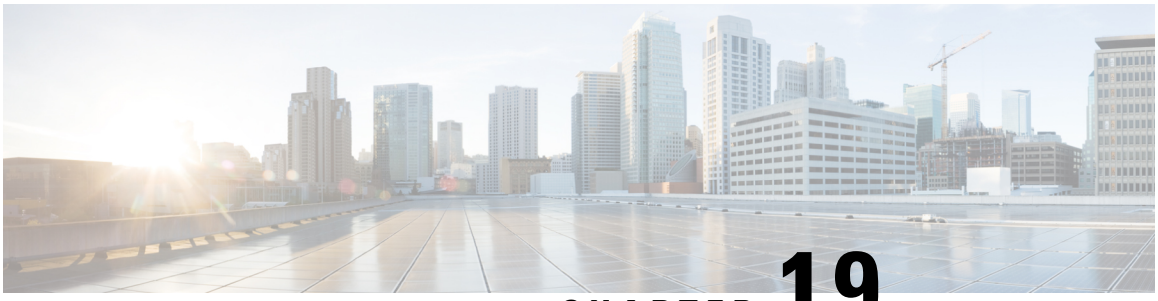
   The **License End Date** column displays the expiry date for the Interconnect Connection license.

   For an AWS hosted connection, Cisco SD-WAN Manager displays the following details:

   - The **AWSHC License UUID** column displays the SKU UUID for the supplemental AWS hosted connection license. On the **Account Licenses** page, use this SKU UUID to view more information about the license SKU.
   - the **AWSHC License End Date** column displays the expiry date for the supplemental AWS hosted connection license.

Related Topics

View Licenses Associated with a Megaport Account, on page 421



CHAPTER 19

Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

Table 79: Feature History

Feature Name	Release Information	Description
Software-Defined Interconnects Megaport	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance as the interconnect gateway in the Megaport fabric and connect an Cisco Catalyst SD-WAN branch location to the interconnect gateway. From the interconnect gateway, you can create software-defined interconnects to an AWS Cloud OnRamp or another interconnect gateway in the Megaport fabric.
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport: Interconnects to Google Cloud and Microsoft Azure	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance as the interconnect gateway in the Megaport fabric and connect a Cisco Catalyst SD-WAN branch location to the interconnect gateway. From the interconnect gateway, you can create software-defined interconnects to Google Cloud VPCs, or Microsoft Azure VNets or Virtual WANs to link your branch location to the cloud resources through the Megaport fabric.

Feature Name	Release Information	Description
Encrypted Multicloud Interconnects with Megaport	Cisco vManage Release 20.9.1	You can extend the Cisco Catalyst SD-WAN fabric from the Interconnect Gateway in Megaport into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers. You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager.

Feature Name	Release Information	Description
Modify Additional Properties of Interconnect Connections to AWS and Microsoft Azure	Cisco vManage Release 20.10.1	

Feature Name	Release Information	Description
		Interconnect Connections to AWS: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwidth of a hosted VIF connection after it is created. Properties of hosted connections cannot be edited after connection creation. With this feature, edit additional properties of both hosted VIF and hosted connections after connection creation. For a full list of editable properties, see Table 82: Editable Properties of Interconnect Connections to AWS, on page 487. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VPC tag that is associated with a connection. With this feature, to attach VPCs to or detach VPCs from a Private Hosted VIF, Private Hosted Connection, or a Transit Hosted Connection, edit the VPC tags associated with the connection to add or remove VPCs. Interconnect Connections to Microsoft Azure: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwith of a connection after it is created. Other properties of a connection are not editable. With this feature, edit additional properties of both Microsoft peering and private peering connections. For a full list of editable properties, see Table 84: Editable Properties of Interconnect Connections to Microsoft Azure, on page

Feature Name	Release Information	Description
		489. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VNet tag that is associated with a connection. With this feature, to attach VNets to or detach VNets from a Private Peering Connection, edit the VNet tags associated with the connection to add or remove VNets.
Audit Management	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The audit management feature helps in understanding if the interconnect cloud and provider connection states are in sync with the Cisco SD-WAN Manager connection state. The State refers to the various connection statuses that Cisco Catalyst SD-WAN establishes with cloud services and providers. The audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what is realized in the cloud.

- Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 429
- Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 430
- Information About Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 436
- Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 438
- Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Megaport, on page 440
- Create Interconnects to AWS, on page 446
- Create Interconnects to Google Cloud, on page 462
- Create Interconnects to Microsoft Azure, on page 471
- Create Interconnect Between Interconnect Gateways, on page 484
- Verify and Modify Configuration, on page 486
- Audit Management, on page 492
- Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Megaport, on page 493

Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

- Create Megaport account.

As part of the ordering process on Cisco Commerce workspace, you receive an email from Megaport about creating your account. Refer to the email for more information.

- For a connection that requires a public peering between an Interconnect Gateway and a Cloud provider, specify a public BGP ASN and a public BGP peering IP address. Ensure that your organization is permitted to use the public BGP ASN and the public BGP peering IP address before you create the connection.
- Ensure you have UUIDs for the required number of Cisco Catalyst 8000v instances that you wish to deploy as Interconnect Gateways.
- Ensure that Cisco SD-WAN Manager can connect to the Internet.

  As part of the configuration workflows, Cisco SD-WAN Manager connects to the Megaport portal via the Internet.

Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

General Restrictions

- At each location, at a time, you can perform only a single interconnect operation such as deploying an Interconnect Gateway, or creating or deleting a connection at a time.
- All interconnect and cloud operations are time bound. If an operation times out, Cisco SD-WAN Manager reports a failure. Currently, the time out values are not configurable.
- If you modify the Global Settings, the changes are applied to any new gateways or connections created after the modification. The changes do not affect gateways or connections created before the modification.
- Cloud Service Provider allocations apply to all Interconnect cloud connections created from Cisco SD-WAN Manager.
- From Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, for a transit-hosted connection, in an AWS region, you can associate only one transit gateway with a Direct Connect gateway.

  While Cisco SD-WAN Manager enforces this restriction from Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, we recommend that you associate only one transit gateway with a Direct Connect gateway in an AWS region with Cisco vManage Release 20.9.1 and earlier releases.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco Catalyst SD-WAN Cloud Interconnect with Megaport is supported only on versions Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.2, any transit gateway created as part of the multicloud workflow is not listed under the transit connections of SDCI workflow.

Interconnects to AWS

- While creating a connection to an AWS cloud resource, adhere to the AWS quotas and limitations. Cisco SD-WAN Manager does not enforce all the AWS quotas and limitations.
- You cannot use cloud resources belonging to different AWS accounts as part of a single connection.

- Attach either private VIFs or transit VIFs to a Direct Connect gateway. You cannot attach a combination of private VIFs and transit VIFs to the same Direct Connect gateway.
- Megaport AWS private hosted VIF connection fails if direct gateway BGP ASN is more than 4200000000.
- From Cisco vManage Release 20.9.2, for a transit-hosted connection, in an AWS region, you can associate only one transit gateway with a Direct Connect gateway.

  While Cisco SD-WAN Manager enforces this restriction from Cisco vManage Release 20.9.2, we recommend that you associate only one transit gateway with a Direct Connect gateway in an AWS region with Cisco vManage Release 20.9.1 and earlier releases.
- All connections to a particular VPC must
  - peer with the same Direct Connect gateway
  - have the same transit gateway or virtual private gateway attachment
- For a transit VIF, the transit gateway and Direct Connect gateway must use different BGP ASNs.
- With Cisco vManage Release 20.5.1, you cannot edit a connection after its creation.

  From Cisco vManage Release 20.6.1, you can modify the bandwidth of hosted VIF connections created earlier. However, you cannot modify the bandwidth of hosted connections after they have been created.
- While creating host VPC tags, choose to use the tag with either the AWS Multi Cloud workflow or the Interconnect Connectivity workflow. This choice cannot be altered after the tag is created and persists till the deletion of the tag.
- Cisco vManage Release 20.9.x and earlier: A host VPC tag selected for Interconnect Connectivity cannot be edited while the tag is in use.

  From Cisco vManage Release 20.10.1: A host VPC tag selected for Interconnect Connectivity can be edited while the tag is in use to add or remove host VPCs.
- Cisco vManage Release 20.9.x and earlier: If a host VPC is associated with a tag and the tag is used in configuring an Interconnect Connection, the host VPC cannot be dissociated from the tag and associated with another tag.

  From Cisco vManage Release 20.10.1: If a host VPC is associated with a tag and the tag is used in configuring an Interconnect Connection, you can dissociate the host VPC from the tag if one or both of the following conditions are met:
  - Additional host VPCs are associated with the tag
  - Additional VPC tags are used in configuring the Interconnect Connection

  After a host VPC is dissociated from a tag, it can be associated with another tag.

  If a VPC tag is used in configuring an Interconnect Connection, you can associate more host VPCs with the tag provided that these host VPCs belong to the same regions as the host VPCs already associated with the tag.
- While creating a Direct Connect Private Hosted VIF, a Direct Connect Private Hosted Connection, or a Direct Connect Transit Hosted Connection to an AWS Direct Connect Gateway from an Interconnect Gateway, you can specify a custom IP address for BGP peering or let Cisco SD-WAN Manager pick an IP address from an internally reserved pool.

In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the subnet 198.18.0.0/16. Before upgrading Cisco SD-WAN Manager from release 20.5.x to 20.6.1 or later, check if any connection to AWS is configured to use a custom BGP peering IP address from the subnet 198.18.0.0/16, which is internally reserved from Cisco vManage Release 20.6.1. If so, delete the connection and re-create the connection with a custom IP address that does not overlap with 198.18.0.0/16.

- When editing interconnect transit connection, if a new transit gateway is selected without a VPC tag in the same region, connection edit is discarded.

Interconnects to Microsoft Azure

- While creating host VNet tags, choose to use the tag with either the Microsoft Azure Multi Cloud workflow or the Interconnect Connectivity workflow. This choice cannot be altered after the tag is created and persists till the deletion of the tag.
- Cisco vManage Release 20.9.x and earlier: A host VNet tag selected for Interconnect Connectivity cannot be edited after creation.

  From Cisco vManage Release 20.10.1: A host VNet tag selected for Interconnect Connectivity can be edited while the tag is in use to add or remove host VNets.
- Cisco vManage Release 20.9.x and earlier: If a host VNet is associated with a tag and the tag is used in configuring an Interconnect Connection, the host VNet cannot be dissociated from the tag in use and associated with another tag.

  From Cisco vManage Release 20.10.1: If a host VNet is associated with a tag and and the tag is used in configuring an Interconnect Connection, the host VNet can be dissociated from the tag if one or both of the following conditions are met:
  - Additional host VNets are associated with the tag
  - Additional VNet tags are used with the Interconnect Connection

  After a host VNet is dissociated from a tag, it can be associated with another tag.

  If a VNet tag is used in configuring an Interconnect Connection, you can associate more host VNets with the tag provided that these host VNets belong to the same regions as the host VNets already associated with the tag.
- While creating a private-peering connection to a Microsoft Azure ExpressRoute from an Interconnect Gateway, you can attach to the connection only the VNets, virtual WANs, and virtual hubs that belong to the same resource group as the ExpressRoute circuit. Attaching VNets, virtual WANs, and virtual hubs from a different resource group is not a supported configuration.

Interconnects to Google Cloud

- Each Cloud Router uses the same ASN for all its BGP sessions.

Restrictions for Encrypted Multicloud Interconnects

Minimum supported release: Cisco vManage Release 20.9.1

Interconnects to AWS

- As per AWS requirement,
  - The minimum instance type must be x-large for Cloud Gateways.
  - A maximum of 10 Cloud Gateways can be attached to a single interconnect connection.
  - One Cloud Gateway can be connected to 30 interconnect connections.

Interconnects to Microsoft Azure

- A single Cloud Gateway can be attached to 8 different cloud interconnect connections and one interconnect connection can connect to 5 different Cloud Gateways.
- To connect to Cloud Gateways in different regions, the express route circuit must be of Premium type.
- For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway and Cloud Gateway.

Interconnects to Google Cloud

- Cloud Interconnect connection to Google Cloud Gateway is supported only with redundancy enabled.
- Only one Google Cloud Gateway can be attached to a single connection.
- Existing Google Cloud Gateways are not supported for cloud interconnects.
- A maximum of 5 Google Cloud Routers can be created for a combination of region and network.

Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

Table 80: Connection Configuration Limits

Description	Count
Interconnect Gateway	
Maximum number of connections (VXC) per Interconnect Gateway	15 **Note**: Aggregate VXC bandwidth should not exceed the bandwidth capacity of the Interconnect Gateway.
Interconnects to AWS	
Maximum number of VPCs per connection to AWS for a private VIF	10
Number of VPCs per connection to AWS for a transit VIF	Default: 15 Maximum: 15000

Description	Count
Maximum number of transit gateways per connection to AWS for a transit VIF	3
Maximum number of Direct Connect gateways per connection	1
Maximum number of VIFs (private or transit) per AWS Direct Connect gateway	Default: 30 Limit can be increased on request.
Maximum number private, public, or transit VIFs per AWS Direct Connect hosted connection	1
Maximum number of prefixes from branch location to AWS for a transit VIF	100
Interconnects to Microsoft Azure	
Maximum number of Interconnect Gateways that can connect to an ExpressRoute	2
Maximum number of VNets to which an ExpressRoute can connect	10
Maximum number of ExpressRoutes that can connect to a VNet	4
Maximum number of ExpressRoutes that can connect to a virtual hub	8 per peering location
Maximum aggregate throughput per virtual WAN ExpressRoute gateway	20 Gbps
Maximum number of VNets that can connect to a virtual hub	500 - (total number of virtual hubs in the virtual WAN)

Interconnects to AWS

- When you delete a connection to AWS, Cisco SD-WAN Manager deletes the VIF, the virtual private gateway, and the route table that were created while establishing the connection.
- When you delete a connection, Cisco SD-WAN Manager removes any attachments and associations to a Direct Connect gateway, transit gateway, or virtual private gateway that were created while establishing the connection.
- While creating a connection to AWS, if you created a Direct Connect gateway or transit gateway from Cisco SD-WAN Manager, deleting the connection does not delete the gateway. Manage these AWS resources as required.
- When you create a connection, a new route table is created and set as the Main route table for the host VPCs attached to the connection.

In Cisco vManage Release 20.5.1, a default route to the virtual private gateway or transit gateway is created in the Main route table and route propagation is enabled. Edit the routes and propagation as required.

From Cisco vManage Release 20.5.1, the static routes and subnet associations required to be accessed by the interconnect should be moved to the newly created Main route table by Cisco SD-WAN Manager.

From Cisco vManage Release 20.6.1, a default route is created in the Main route table to only the transit gateway, and route propagation is enabled. Edit the routes and propagation as required.

- If you modify the Global Settings, the changes are applied to any new gateways or connections created after the modification. The changes do not affect gateways or connections created before the modification.

Interconnects to Google Cloud

- For nonredundant connectivity, you must deploy a Google Cloud Router in each network-region and create a VLAN attachment for each Google Cloud Router. In the Megaport fabric, an interconnect is created from the Interconnect Gateway to each Google Cloud Router.
- For redundant connectivity, you must deploy two Google Cloud Routers in each network-region and create a VLAN attachment for each Google Cloud Router. In the Megaport fabric, an interconnect is created from each of a pair of Interconnect Gateways to each Google Cloud Router.
- For use with interconnect attachments, you must set the Google ASN for the Google Cloud Routers to 16550.

Interconnects to Microsoft Azure

- Only one pair of Interconnect Gateways can connect to a particular ExpressRoute to provide a HA connection to the VNet attched to the ExpressRoute.

  To connect a second pair of Interconnect Gateways to the same vNet, do as follows: create another ExpressRoute; attach the vNet to the ExpressRoute; and connect the Interconnect Gateways to the ExpressRoute

  You can have a maximum four such ExpressRoutes connecting to a VNet, and connect each Express Route to a pair of Interconnect Gateways.

- An ExpressRoute can connect to maximum of 10 VNets. You can attach VNets to an ExpressRoute while creating connections to the ExpressRoute from Interconnect Gateways. VNets are attached based on the VNet tags you choose for the connection.

  If you choose a VNet tag that applies to more than 10 VNets or choose a combination of VNet tags so that the total number of select VNets is more than 10, interconnect creation fails.



Note Any VNets that you may have attached to the ExpressRoute from the Azure portal are also considered while determining the number VNets that you can attach to the ExpressRoute while creating the connection from the interconnect gateways.

- In the Azure portal, if cloud gateway extension connections intended for one ExpressRoute gateway also appear in a second ExpressRoute gateway, create two ExpressRoute gateways with a different prefix.

- You can connect a VNet to either a VNet gateway or an ExpressRoute gateway. So, if you have created a private peering to a VNet through a VNet gateway, you cannot create a private peering to the same VNet through an ExpressRoute gateway, and vice-versa.
- If a VNet is connected to virtual hub in a virtual WAN, the same VNet cannot be connected to another virtual WAN.
- Each region of a virtual WAN must have only one virtual hub.
- All the VNets in a region must connect to a single virtual hub in the same region.
- Redundant connectivity is the default and only supported configuration. You must create connections to Microsoft Azure from a pair of Interconnect Gateways in the Megaport fabric.

  When choosing a pair of Interconnect Gateways from which you wish to create the primary and secondary connections to a Microsoft Azure ExpressRoute, ensure that the Interconnect Gateways are configured to use the same BGP ASN for BGP peering.

Information About Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance in the fabric of the SDCI provider Megaport. Further, you can link a branch location to the Cisco Catalyst 8000v instance using the Cisco Catalyst SD-WAN fabric. We recommend that you deploy the Cisco Catalyst 8000v instance at a Megaport location closest to your branch location.

The Cisco Catalyst 8000v instance acts as an edge device in the Cisco Catalyst SD-WAN fabric and as the Interconnect Gateway in the Megaport fabric. From the Interconnect Gateway, you can create a direct Layer 2 connection (an interconnect) in the Megaport fabric to a cloud onramp or another Interconnect Gateway. The interconnects link branch locations, or link branch locations to cloud service providers through the Megaport fabric.



Note In the Megaport terminology, the interconnect gateway is also referred to as the Megaport Virtual Edge (MVE). The direct Layer 2 connection from an interconnect gateway to a Cloud OnRamp or another interconnect gateway is called a Virtual Cross Connect (VXC).

In this setup, Cisco Catalyst SD-WAN fabric acts as the overlay network, and the Megaport fabric acts as the underlay network. The Megaport fabric provides data-center-agnostic, efficient, high-speed, low-latency, high-bandwidth connectivity across data centers in 700 global locations.

You can create the following types of connections from an Interconnect Gateway:

Table 81: Connection Types

Destination	Connection Types	From Release
Amazon Web Services	• Direct Connect - Public Hosted Virtual Interface (VIF) • Direct Connect - Private Hosted VIF • Direct Connect - Public Hosted Connection • Direct Connect - Private Hosted Connection • Direct Connect - Transit Hosted Connection	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1
Google Cloud	Partner Interconnect Attachment to a Google Cloud Router	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1
Microsoft Azure	• Partner ExpressRoute Circuit - Microsoft Peering • Partner ExpressRoute Circuit - Private Peering	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1
Interconnect Gateway	Link between Cisco Catalyst SD-WAN Branch Locations connected to the Interconnect Gateways	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1

Cisco SD-WAN Manager enables you to

- Configure and deploy the Cisco Catalyst 8000v instance at a Megaport location
- Create software-defined cloud interconnects to public or private clouds
- Create interconnects to link Cisco Catalyst SD-WAN branch locations across the Megaport fabric

Support is offered along with this solution. Contact Cisco Support for any questions or issues regarding this solution.

Benefits of Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

1. Branch locations connect seamlessly to the Megaport fabric over the Cisco Catalyst SD-WAN fabric.
2. Interconnects to public or private cloud with assured SLAs.
3. End-to-end traffic security, segmentation, and policy through the Cisco Catalyst SD-WAN fabric.
4. Cisco is the single point of contact for billing, provisioning, and support.
5. Cisco SD-WAN Manager provides a single pane to manage your connectivity to any cloud.

6. End-to-end visibility across the Cisco Catalyst SD-WAN fabric and the Megaport SDN.
7. Data-center-agnostic links between Cisco Catalyst SD-WAN branch locations and between Cisco Catalyst SD-WAN branch locations and a public or private cloud.

Encrypted Multicloud Interconnects

Minimum supported release: Cisco vManage Release 20.9.1

You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager. You can terminate the virtual cross connects from the Interconnect Gateway in the cloud interconnect provider to the existing Cloud Gateways which are created as part of the Multicloud workflow. For more information, see Cloud OnRamp for Multicloud, on page 305. This feature enables support for both internet and private paths to access VPC and VNET workloads.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, encrypted multicloud interconnects supports AWS Cloud Gateway using Cloud WAN solution.

Benefits

- Provides end to end encryption from branch sites to Cloud Gateways through the cloud interconnect provider backbone.
- Supports multiple VPN segments over single virtual cross connect.
- Supports modification of VPC and VNET tags before and after the connection creation. VPN to VPC or VNET tag mapping can be performed using the Multicloud Intent Management screen.
- Route advertisements are controlled by Interconnect Gateways and Cloud Gateways to overcome prefix advertisements restrictions imposed by cloud service providers.

Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

Prerequisite Configuration

1. Create Megaport account.

   As part of the ordering process on Cisco Commerce Workspace (CCW), you receive an email from Megaport about creating your account. Refer to the email for more information.
2. Associate Megaport account with Cisco SD-WAN Manager.
3. Configure Global Settings for Interconnect Gateways.
4. Create necessary network segments (see Segmentation Configuration Guide).
5. Ensure you have UUIDs for the required number of Cisco Catalyst 8000v instances that you wish to deploy as Interconnect Gateways.
6. Attach Megaport Template to a Cisco Catalyst 8000v instance.

7. Create Interconnect Gateway at Megaport location closest to your Cisco Catalyst SD-WAN branch location.

   For connectivity to AWS, create an Interconnect Gateway at the Megaport location.

   For redundant connectivity to Google Cloud, create a pair of Interconnect Gateways in the Megaport fabric. For nonredundant connectivity, deploy an Interconnect Gateway at a Megaport location.

   For connectivity to Microsoft Azure, create a pair of Interconnect Gateways in the Megaport fabric. Redundant connectivity is the default and only supported configuration.

   For connectivity between Cisco Catalyst SD-WAN branch locations, for each branch location, create an Interconnect Gateway at the closest Megaport location.

Workflow to Create Interconnect to AWS

Before you perform the following configuration procedures, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Associate AWS account with Cisco SD-WAN Manager.
2. Discover Host Private Networks to connect to AWS Virtual Private Clouds (VPCs).
3. Create one of the following types of connection:

Connection Type	Tip
Direct Connect - Public Hosted Virtual Interface (VIF)	Use this connection for a link to a public AWS resource, with the link having a bandwidth between 50 Mbps and 1 Gbps.
Direct Connect - Private Hosted VIF	Use this connection for a dedicated link to an AWS VPC, with the link having a bandwidth between 50 Mbps and 1 Gbps. **Note**: Bandwidth of a connection must not exceed the purchased entitlement.
Direct Connect - Public Hosted Connection	Use this connection for a link to a public AWS resource, with the link having a fixed bandwidth of more than 1 Gbps.
Direct Connect - Private Hosted Connection	Use this connection for a dedicated link to an AWS VPC, with a link bandwidth of more than 1 Gbps.
Direct Connect - Transit Hosted Connection	Use this connection for dedicated links to up 5,000 AWS VPCs via a transit gateway, with a link bandwidth of more than 1 Gbps. You can attach up to three transit gateways to a Direct Connect gateway and connect to up to 15,000 VPCs.

Workflow to Link Cisco Catalyst SD-WAN Branch Locations

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

- Create an Interconnect between the Interconnect Gateways.

Workflow to Create Interconnect to Google Cloud

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Create the required VPC network using the Google Cloud portal.
2. Deploy Google Cloud Routers in network-regions to which you wish to connect.

   For nonredundant connectivity, using the Google Cloud portal, deploy a Google Cloud Router in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   For redundant connectivity, using the Google Cloud portal, deploy two Google Cloud Routers in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.
3. Associate Google Cloud account with Cisco SD-WAN Manager.
4. Create Interconnects to Google Cloud Routers from Interconnect Gateways

Workflow to Create Interconnect to Microsoft Azure

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Associate Microsoft Azure account with Cisco SD-WAN Manager.
2. Create the required Azure ExpressRoute circuits.
3. Discover Host Private Networks to connect to Azure Virtual Networks (VNets).
4. Create one of the following types of connection:
   - Public Peering Connection to an Azure ExpressRoute
   - Private Peering Connection to an Azure ExpressRoute

Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Megaport

Associate Megaport Account with Cisco SD-WAN Manager

Prerequisite

Create Megaport account. As part of the ordering process on Cisco Commerce Workspace (CCW), you receive an email from Megaport about creating your account. Refer to the email for more information.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Associate Interconnect Account**.
4. Configure the following:

Interconnect Provider	Choose **Megaport**.
Account Name	Enter a name of your choice. This name is used to identify the Megaport account in workflows that define the cloud or site-to-site interconnects. **Note** Starting from Cisco vManage Release 20.6.1, spaces are not allowed in Account Name. If you are upgrading Cisco SD-WAN Manager from Cisco vManage Release 20.5.1 to Cisco vManage Release 20.6.1, remove the spaces in your Account Name or replace the spaces with '_'.
Description (Optional)	Enter a description.
User Name	Enter the username of your Megaport account.
Password	Enter the password of your Megaport account.

5. Click **Add**.

Cisco SD-WAN Manager authenticates the account and saves the account details in a database.

Configure Global Settings for Interconnect Gateways

Prerequisites

1. Create a Megaport account. As part of the ordering process on Cisco Commerce Workspace (CCW), you receive an email from Megaport about creating your account. Refer to the email for more information.
2. Associate Megaport account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Global Settings**.
   a. To add global settings, click **Add**.
   b. To modify global settings, click **Edit**.
4. Configure the following:

Enable Configuration Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default. **Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables it for all other multicloud and interconnect providers.

Interconnect Provider	Choose **Megaport**.
Software Image	Choose a Catalyst 8000v image.
Instance Size	Instance Size determines the compute footprint and throughput of each Cisco Catalyst 8000v instance.
Interconnect Transit Color	Choose the color to be assigned for connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.
Interconnect CGW SDWAN Color	Minimum supported release: Cisco vManage Release 20.9.1 Choose the color to be used for the interface through which the Interconnect Gateway connects to the Cloud Gateway. **Note** Color assigned to an interface must be unique for the Interconnect Gateway devices and common across Cloud Interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway, and Cloud Gateway.

5. To save the newly added global settings, click **Save**.

   To save the modified global settings, click **Update**.

Attach Megaport Template to Cisco Catalyst 8000v Instance



Note This procedure is not required if you enabled configuration groups. In this case, skip to Create Interconnect Gateway at a Megaport Location.

Before you can deploy a Cisco Catalyst 8000v instance as an Interconnect Gateway at a Megaport location, you must attach the Megaport default template to the device. We recommend that you attach the template named *Default_MEGAPORT_ICGW_C8000V_Template_V01*.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Device Templates**.



Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

3. Choose the **Template Type** as **Default** and find the template named *Default_MEGAPORT_ICGW_C8000V_Template_V01*.
4. For the template, click **...** and click **Attach Devices**.
5. Choose the Cisco Catalyst 8000v instance from **Available Devices** and move it to **Selected Devices**. Click **Attach**.
6. Configure the following and click **Next**.
   - Color
   - Hostname
   - System IP
   - Site ID
7. Click **Configure Devices**.

Create an Interconnect Gateway at a Megaport Location

Deploy a Cisco Catalyst 8000v instance as the interconnect gateway at the desired Megaport location. We recommend that you deploy the Cisco Catalyst 8000v instance at the Megaport location closest to your branch location.

Before You Begin

1. Associate a Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Attach a Megaport template to a Cisco Catalyst 8000v instance, if you do not wish to enable configuration groups.
4. If you enable configuration groups, ensure that you configure device parameters for devices that are associated with the configuration group.
5. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the Interconnect Gateway. Without the required license, Interconnect Gateway creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Create an Interconnect Gateway at a Megaport Location

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Create Interconnect Gateway**.

4. Configure the following:

Interconnect Provider	Choose **Megaport**.
Gateway Name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.
Account Name	Choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager. (Minimum release: Cisco vManage Release 20.9.1) To view the Interconnect Gateway licenses associated with the account, click **Check available licenses**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Megaport location where the Cisco 8000v instance must be deployed.
Provider License Type	(Minimum release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Choose one of the following: • **Prepaid**: Choose a prepaid license type to create the interconnect gateway. Before Cisco Catalyst SD-WAN Manager Release 20.14.1, by default, only the prepaid license type was available. • **PayG**: Choose a pay-as-you-go (PAYG) license type to create the interconnect gateway.
IP Transit	(Minimum release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Choose the IP transit bandwidth value.
NHM Region	(Minimum release: Cisco Catalyst SD-WAN Manager Release 20.14.1) From the drop-down list, choose a network health monitoring (NHM) region for which you want to create the interconnect gateway.
Site Name	(Minimum release: Cisco vManage Release 20.10.1) From the drop-down list, choose a site for which you want to create the interconnect gateway.

Configuration Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups. **Note** The **Configuration Group** drop-down list includes only configuration groups that you create from this drop-down list. It does not include other configuration groups that are created in Cisco Catalyst SD-WAN. The configuration groups in this drop-down list include the options that are needed for this provider.
Chassis Number	Choose the chassis number of a Cisco Catalyst 8000v instance that has the Megaport default template attached. **Note** From Cisco vManage Release 20.10.1, the chassis numbers are auto-populated when you choose a site from the **Site Name** drop-down list.
Instance Settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect Global Settings. • **Custom**: Choose a specific instance size and software image for this gateway.
MRF Role	(Minimum release: Cisco vManage Release 20.10.1) Choose a router role: **Border** or **Edge**. This option is available only when Multi-Region Fabric is enabled.
Transport Gateway	(Minimum release: Cisco vManage Release 20.10.1) Choose **Enabled** or **Disabled**. This option is available only when Multi-Region Fabric is enabled.

5. Click **Add**.

When the configuration task is successful, the interconnect gateway is listed in the **Gateway Management** page.

Create Interconnects to AWS

Associate AWS Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud**.
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Amazon Web Services**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Log in to AWS with	Choose **Key** or **IAM Role**.
Role ARN	Enter the API/Secret Key or the Role ARN.

5. Click **Add**.

Cisco SD-WAN Manager uses the API/Secret Key or the Role ARN to authenticate the user account with AWS as part of the API workflow to create connections to AWS.

Discover Host Private Networks and Tag AWS VPCs

A number of host VPCs can be grouped together using a tag. VPCs under the same tag are considered as a singular unit. Tag the AWS VPCs to which you wish to create software-defined cloud interconnects from an Interconnect Gateway.

Prerequisite

Associate AWS Account with Cisco SD-WAN Manager.

Add a Tag

Group VPCs and tag them together.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Amazon Web Services**.

   The available host VPCs are discovered and listed in a table.
5. Select the VPCs that you wish to tag using the check boxes in the left-most column.

6. Click **Tag Actions**.
7. Click **Add Tag** and configure the following:

Field	Description
Tag Name	Enter a name for the tag that links the selected VPCs.
Region	List of regions that correspond to the selected VPCs. Click **X** to omit a region and associated VPCs from the tag.
Selected VPCs	List of VPC IDs of the selected host VPCs. Click **X** to omit a VPC from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	To use the VPC tag while creating a cloud interconnect connection to AWS, check the check box. If enabled, the tag can only be used for Cloud Interconnect connections and is not available for Multicloud Gateway Intent Mapping. If you do not check the check box, you cannot use the VPC tag to create a Cloud Interconnect connection. **Note** Do not enable this setting when you use Cloud Gateways to connect VPC workloads. You cannot edit this setting when the tag is in use by a connection.

8. Click **Add**.

On the **Discover Host Private Networks** page, the VPCs you selected are tagged and the tag name is shown in the **Host VPC Tag** column. If you chose to use the VPC tag for software-defined cloud interconnects, the **Interconnect Enabled** column reads **Yes**.

Edit a Tag

Add VPCs to or remove VPCs from an existing tag.

From Cisco vManage Release 20.10.1, edit a VPC tag associated with an Interconnect Connection subject to the following conditions:

- If only one VPC is associated with a VPC tag, you cannot remove the VPC from the tag. To remove the VPC from the tag, delete the Interconnect Connection and then edit the tag.
- For a Transit Hosted Connection, the VPCs you wish to associate with a tag must be from the same regions as the VPCs already associated with the tag.

  To attach VPCs from a new region to the Transit Hosted Connection, do the following:

  1. Create a new tag for the region and associate required VPCs.
  2. Edit the Transit Hosted Connection and attach the VPC tag to the connection.

- For a private VIF or private hosted connection, you can associate VPCs from a new region while editing the tag.

Note In Cisco vManage Release 20.9.1 and earlier releases, you cannot edit a VPC tag that is associated with an Interconnect Connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Amazon Web Services**.

   The available host VPCs are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Edit Tag** and modify the following as required:

Field	Description
Tag Name	From the drop-down list, choose a tag name.
Region	This field shows the list of regions that correspond to the VPCs associated with the tag. • Choose additional regions from the drop-down list. • Click **X** to omit a region and associated VPCs from the tag.
Selected VPCs	This field shows the list of VPCs associated with the tag. • Choose additional VPCs from the drop-down list. • Click **X** to omit a VPC from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	(Read only) Indicates whether the VPC is configured to be used while configuring Interconnect Connections or for Multicloud Gateway intent mapping.

7. Click **Update**.

Delete a Tag

Remove a tag that groups together VPCs.

Note You cannot delete a VPC tag while the tag is associated with an Interconnect Connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Amazon Web Services**.

   The available host VPCs are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Delete Tag**.
7. **Tag Name**: From the drop-down list, choose a tag name.
8. Click **Delete**.

Create Direct Connect Public Hosted VIF to AWS from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Attach Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateway at a Megaport Location.
7. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.

6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
Connection Type	Choose **Hosted VIF**.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

10. Configure the following and click **Next**:

VIF Type	Choose **Public**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Interconnect IP Address	Enter the public IP Address (CIDR) to be used as the BGP Peer ID of the Interconnect Gateway.
Amazon IP Address	Enter the public IP Address (CIDR) to be used as the AWS BGP Peer ID.
Prefixes	Enter the summary addresses and prefixes you wish to advertise to AWS.
Segment	Choose the segment ID for this connection.

11. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Private Hosted VIF to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateway at a Megaport Location.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.

Connection Type	Choose **Hosted VIF**.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

10. Configure the following and click **Next**:

VIF Type	Choose **Private**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location. **Note** We recommend not to use any AWS GovCloud locations for non AWS GovCloud accounts.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Direct Connect Gateway	**a.** Click the Refresh button to fetch the Direct Connect gateways associated with the selected AWS account. **b.** Choose the Direct Connect Gateway to which the Direct Connect connection must be created. Alternatively, create a new Direct Connect Gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.

Settings	Choose one of the following: • **Global**: • BGP peering IP address is picked from an internally reserved /16 subnet. In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the subnet 198.18.0.0/16. • BGP ASN is picked from the Global Settings. • **Custom**: • Enter a custom /30 CIDR IP address for BGP peering. • Enter custom BGP ASN for peering. • Beginning with Cisco vManage Release 20.8.1: • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. • The custom subnet must be specified as /30. • The custom subnet should not conflict with 172.31.251.0/21. • The custom subnet must not conflict with the subnets used for other connections. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.
Segment	Choose the segment ID for this connection.

Attachment	Cisco vManage Release 20.8.1 and earlier: Choose **VPC**. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection.
	Cisco vManage Release 20.9.1 and later: Choose one of the following: • **VPC** **Segment**: Choose the segment ID for this connection. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. • **Cloud Gateway** **Cloud Gateways**: Choose the Cloud Gateways to attach to this connection. If the drop-down is empty, you must first create the cloud gateway using the Multicloud workflows. For a single connection, AWS supports up to 10 Cloud Gateways. Each Cloud Gateway can be connected to 30 Interconnect Connections.

11. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Public Hosted Connection to AWS from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Attach Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateway at a Megaport Location.
7. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.



Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
Connection Type	Choose **Hosted Connection**.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco vManage.

10. Configure the following and click **Next**:

Connection VIF Type	Choose **Public**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Interconnect IP Address	Enter the public IP Address (CIDR) to be used as the BGP Peer ID of the Interconnect Gateway.
Amazon IP Address	Enter the public IP Address (CIDR) to be used as the AWS BGP Peer ID.
Prefixes	Enter the summary AWS addresses and prefixes you wish to advertise to the branch location.

Segment	Choose the segment ID for this connection.

11. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Private Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateway at a Megaport Location.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.



Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.

7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
Connection Type	Choose **Hosted Connection**.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

10. Configure the following and click **Next**:

Connection VIF Type	Choose **Private**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location. **Note** We recommend not to use any AWS GovCloud locations for non AWS GovCloud accounts.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.
Direct Connect Gateway	**a.** Click the Refresh button to fetch the Direct Connect gateways associated with the selected AWS account. **b.** Choose the Direct Connect Gateway to which the Direct Connect connection must be created. Alternatively, create a new Direct Connect Gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.

Settings	Choose one of the following: • **Global**: • BGP peering IP address is picked from an internally reserved /16 subnet. In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the subnet 198.18.0.0/16. • BGP ASN is picked from the Global Settings. • **Custom**: • Enter a custom /30 CIDR IP address for BGP peering. • Enter custom BGP ASN for peering. • Beginning with Cisco vManage Release 20.8.1: • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. • The custom subnet must be specified as /30. • The custom subnet should not conflict with 172.31.251.0/21. • The custom subnet must not conflict with the subnets used for other connections. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.
Segment	Choose the segment ID for this connection.

Attachment	Cisco vManage Release 20.8.1 and earlier: Choose **VPC**. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection.
	Cisco vManage Release 20.9.1 and later: Choose one of the following: • **VPC** **Segment**: Choose the segment ID for this connection. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. • **Cloud Gateway** **Cloud Gateways**: Choose the Cloud Gateways to attach to this connection. If the drop-down is empty, you must first create the cloud gateway using the Multicloud workflows. For a single connection, AWS supports up to 10 Cloud Gateways. Each Cloud Gateway can be connected to 30 Interconnect Connections.

11. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Transit Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and Tag AWS VPCs.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateway at a Megaport Location.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
Connection Type	Choose **Hosted Connection**.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

10. Configure the following and click **Next**:

Connection VIF Type	Choose **Transit**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location. **Note** We recommend not to use any AWS GovCloud locations for non AWS GovCloud accounts.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

Direct Connect Gateway	**a.** Click the Refresh button to fetch the Direct Connect gateways associated with the selected AWS account. **b.** Choose the Direct Connect Gateway to which the Direct Connect connection must be created. Alternatively, create a new Direct Connect Gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.
Settings	Choose one of the following: • **Global**: • BGP peering IP address is picked from an internally reserved /16 subnet. In Cisco vManage Release 20.5.1, the IP address is picked from the subnet 192.168.0.0/16. From Cisco vManage Release 20.6.1, the IP address is picked from the subnet 198.18.0.0/16. • BGP ASN is picked from the Global Settings. • **Custom**: • Enter a custom /30 CIDR IP address for BGP peering. • Enter custom BGP ASN for peering. • Beginning with Cisco vManage Release 20.8.1: • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. • The custom subnet must be specified as /30. • The custom subnet should not conflict with 172.31.251.0/21. • The custom subnet must not conflict with the subnets used for other connections. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.

Segment	Choose the segment ID for this connection.
Attachment	Choose **Transit Gateway**. **Transit Gateway**: **a.** Click the Refresh button to fetch the transit gateways associated with the selected AWS account. **b.** Choose the transit gateway to which the Direct Connect connection must be created. Alternatively, create a new transit gateway by clicking **Add New Transit Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Select **AWS Region**. **d.** Click **Save**. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. Click **Add Prefixes**. Enter the IPv4 CIDR prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard.

11. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Interconnects to Google Cloud

Associate Google Cloud Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud** .
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Google Cloud**.
Cloud Account Name	Enter a name of your choice.

Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Private Key ID	Click **Upload Credential File**. You must generate this file by logging in to the Google Cloud console. The private key ID may be in the JSON or the REST API format. The format depends on the method of key generation. For more details, see Google Cloud documentation.

5. Click **Add**.

Cisco SD-WAN Manager uses the Private Key ID to authenticate the user account with Google Cloud as part of the workflow to create connections to Google Cloud.

Create Interconnect to Google Cloud Routers from Interconnect Gateways

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Deploy Google Cloud Routers in network-regions to which you wish to connect.

   For nonredundant connectivity, on the Google Cloud console, deploy a Google Cloud Router in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   For redundant connectivity, on the Google Cloud console, deploy two Google Cloud Routers in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

Note For use with interconnect attachments, you must set the Google ASN for the Google Cloud Routers to 16550.

3. Associate Megaport Account with Cisco SD-WAN Manager.
4. Configure Global Settings for Interconnect Gateways.
5. Attach Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateway at a Megaport Location closest to your Cisco Catalyst SD-WAN branch location.

   For redundant connectivity to Google Cloud, create a pair of Interconnect Gateways in the Megaport fabric. For nonredundant connectivity, deploy an Interconnect Gateway at a Megaport location.
7. Create necessary network segments (see Segmentation Configuration Guide).
8. Associate Google Cloud Account with Cisco SD-WAN Manager.
9. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.
5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Google Cloud**.
Google Account	Choose a Google account by the account name entered while associating the Google account details with Cisco SD-WAN Manager.
Attachment	Minimum supported release: Cisco vManage Release 20.9.1 Choose **Shared VPC** to attach a Google Cloud Router and Google Cloud Interconnect to the connection.
Region	Minimum supported releases: Cisco vManage Release 20.9.1 Choose a Google Cloud region.
VPC Network	Minimum supported releases: Cisco vManage Release 20.9.1 Choose the VPC network to deploy this connection.

Redundancy	For Cisco vManage Release 20.8.1 and earlier: Choose **Enable** if you want to create connections with redundancy. **Primary Google Cloud Interconnect Attachment:** • Click the refresh symbol next to the **Primary Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*. **Secondary Google Cloud Interconnect Attachment:** • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*. The secondary interconnect attachment options are determined based on the region and network to which the primary interconnect attachment belongs. If you do not have an unused interconnect attachment in the same region and network as the primary interconnect attachment, the drop-down list is empty and indicates that you must create a redundant interconnect attachment on the Google Cloud portal. Choose **Disable** if you want to create the connection without redundancy. **Google Cloud Interconnect Attachment**: • Click the refresh symbol next to the **Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*.

	For Cisco vManage Release 20.9.1 and later: **Google Cloud Router**: • Click the refresh symbol next to the **Google Cloud Router** drop-down list. • Choose a Google Cloud router or click **Add New Google Cloud Router**. If you clicked **Add New Google Cloud Router**, configure the router settings in the **Add Google Cloud Router** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Cloud Router Name: Enter a unique Google Cloud router name. **Note** Google Cloud routers are always created with a BGP ASN of 16550, MTU of 1500 and with default routing enabled. **Google Cloud Interconnect Attachment**: • Click the refresh symbol next to the **Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the router settings in the **Add Google Cloud Interconnect Attachment** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud Interconnect attachment region. • VPC Network: Choose the Google Cloud network for the interconnect attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • IC Attachment Name: Enter a unique name for the interconnect attachment. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.

10. Configure the following settings for the primary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the primary interconnect attachment.
Connection Name	Enter a unique name for the primary connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

11. If you enabled redundancy in Step 8, configure the following settings for the secondary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the secondary interconnect attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary interconnect attachment.
Connection Name	Enter a unique name for the secondary connection.
Bandwidth (Mbps)	Bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which a connection must be established to the secondary interconnect attachment.

12. Configure the following and click **Next**:

Settings	Choose **Auto-generated** or **Custom**. • **Auto-generated:** The Interconnect BGP ASN is selected by the system • **Custom**: Specify Interconnect BGP ASN of your choice for peering with the interconnect virtual cross connect attachments. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. BGP peering IP addresses for interconnects to Google Cloud Routers are auto-assigned by Google from the subnet (169.254.0.0/16). The IP addresses cannot be configured from Cisco SD-WAN Manager.
Segment	Choose a segment ID for this connection.

13. Review the connection summary.

- To create the connection, click **Save**.
- To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched and creates the interconnects between the Interconnect Gateway and the interconnect attachments of the Google Cloud routers.

When the task is successful, the connections are listed on the **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

What to do Next: On the Google Cloud console, manage the routes advertised from the Google Cloud Routers towards the interconnect gateway via BGP.

Create Interconnect Connection to a Cloud Gateway In Google Cloud

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Associate Megaport Account with Cisco SD-WAN Manager.
3. Configure Global Settings for Interconnect Gateways.
4. Attach Megaport Template to Cisco Catalyst 8000v Instance.
5. Create Interconnect Gateway at a Megaport Location closest to your Cisco Catalyst SD-WAN branch location.

   Only redundant connectivity is supported on Google Cloud. You must create a pair of Interconnect Gateways in the Megaport fabric.
6. Create necessary network segments (see Segmentation Configuration Guide).
7. Associate Google Cloud Account with Cisco SD-WAN Manager.
8. Create a Google Cloud Gateway using the Multicloud workflow.
9. Ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.
5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.

6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the connection must be created.
7. To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Google Cloud**.
Google Account	Choose a Google account by the account name entered while associating the Google account details with Cisco SD-WAN Manager.
Attachment	Choose **Cloud Gateway** to connect to a Cloud Gateway. **Cloud Gateways**: You can select only one Cloud Gateway from the drop-down list.

10. Configure the following and click **Next**:

PRIMARY	
Google Cloud Router	Primary Google Cloud router is autopopulated based on the selected Cloud Gateway.
Google Cloud Interconnect Attachment	Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the router settings in the **Add Google Cloud Interconnect Attachment** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud Interconnect attachment region. • VPC Network: Choose the associated network for the interconnect attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network. • IC Attachment Name: Enter a unique attachment name. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.
SECONDARY	
Google Cloud Router	Secondary Google Cloud router is autopopulated based on the selected Cloud Gateway.

Google Cloud Interconnect Attachment	Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the interconnect settings in the **Add Google Cloud Interconnect Attachment** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud Interconnect attachment region. • VPC Network: Choose the associated network for the interconnect attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network. • IC Attachment Name: Enter a unique attachment name. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.

11. Configure the following settings for the primary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the primary interconnect attachment.
Connection Name	Enter a unique name for the primary connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

12. Configure the following settings for the secondary virtual cross connect attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Megaport location closest to the Google Cloud region where you created the Google Cloud Router and the secondary interconnect attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary interconnect attachment.
Connection Name	Enter a unique name for the secondary connection.
Bandwidth (Mbps)	Bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which a connection must be established to the secondary interconnect attachment.

13. Configure the following and click **Next**:

Settings	Choose **Auto-generated** or **Custom**. • **Auto-generated:** The Interconnect BGP ASN is selected by the system • **Custom**: Specify Interconnect BGP ASN of your choice for peering with the interconnect virtual cross connect attachments. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. BGP peering IP addresses for interconnects to Google Cloud Routers are auto-assigned by Google from the subnet (169.254.0.0/16). The IP addresses cannot be configured from Cisco SD-WAN Manager.
Segment	Choose a segment ID for this connection.

14. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

    When you save the connection configuration, a configuration task is launched and creates the interconnects between the Interconnect Gateway and the interconnect attachments of the Google Cloud routers.

    When the task is successful, the connections are listed on the **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

What to do Next: On the Google Cloud console, manage the routes advertised from the Google Cloud Routers towards the interconnect gateway via BGP.

Create Interconnects to Microsoft Azure

Associate Microsoft Azure Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud** .
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Microsoft Azure**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.

Tenant ID	Enter the ID of your Azure Active Directory (AD). **Tip** To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret Key	Enter the password associated with the client ID.

5. Click **Add**.

Discover Host Private Networks and Tag Microsoft Azure VNets

Tag the Microsoft Azure VNets to which you wish to create software-defined cloud interconnects from an interconnect gateway. Azure VNets grouped using the same VNet tag are considered a singular unit.

Prerequisite

Associate Microsoft Azure Account with Cisco SD-WAN Manager.

Add a Tag

Group VNets and tag them together.

Note VNets belonging to different resource groups cannot be used together.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Choose the Azure VNets that you wish to tag by checking the corresponding check boxes.
6. Click **Tag Actions**.
7. Click **Add Tag** and configure the following:

Field	Description
Tag Name	Enter a name for the tag.

Field	Description
Region	If you selected VNets before clicking **Add Tag**, this field shows the list of regions that correspond to the selected VNets. • If you did not select VNets before clicking **Add Tag** or wish to select more regions, choose regions from the drop-down list. • Click **X** to omit a region and associated VNets from the tag.
Selected VNets	If you selected VNets before clicking **Add Tag**, this field shows the list of VNet IDs of the selected host VNets. • If you did not select VNets before clicking **Add Tag** or wish to select more VNets, choose VNets from the drop-down list. • Click **X** to omit a VNet from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	To use the VNets tag while creating interconnect connections to Microsoft Azure, check the check box. If enabled for interconnect connetions, the tag cannot be used in the Microsoft Azure Multicloud workflow. If not enabled for interconnect connections, the tag can only be used with Microsoft Azure Multicloud workflow. **Note** Do not enable this setting when you use Cloud Gateways to connect VNet workloads.

8. Click **Add**.

On the **Host Private Networks** page, the Azure vNets you selected earlier are tagged and the tag name is shown in the **VNET Tag** column. If you chose to use the vNet tag for cloud interconnects, the **Interconnect Enabled** column reads **Yes**.

Edit a Tag

Add VNets to or remove VNets from an existing tag.

From Cisco vManage Release 20.10.1, edit a VNet tag associated with an interconnect connection subject to the following conditions:

- If only one VNet is associated with a VNet tag, you cannot remove the VNet from the tag. To remove the VNet from the tag, delete the interconnect connection and then edit the tag.
- For a private-peering connection with a virtual WAN attachment, the VNets you wish to associate with the tag must be from the same regions as the VNets already associated with the tag.

  To attach VNets from a new region to the private-peering connection, do the following:

  1. Create a new tag for the region and associate required VNets.
  2. Edit the private-peering connection and attach the VNet tag to the connection.

- For a private-peering connection with a VNet attachment, you can associate VNets from a new region to the tag while editing the tag.



Note In Cisco vManage Release 20.9.1 and earlier releases, you cannot edit a VNet tag that is associated with an interconnect connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Edit Tag** and modify the following as required:

Field	Description
Tag Name	From the drop-down list, choose a tag name.
Region	This field shows the list of regions that correspond to the VNets associated with the tag. • Choose additional regions from the drop-down list. • Click **X** to omit a region and associated VNets from the tag.
Selected VNets	This field shows the list of VNets associated with the tag. • Choose additional VNets from the drop-down list. • Click **X** to omit a VNet from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	(Read only) Indicates whether the VNet is configured to be used while configuring interconnect connections or for Multicloud Gateway intent mapping.

7. Click **Update**.

Delete a Tag

Remove a tag that groups together VNets.

Note You cannot delete a VNet tag while the tag is associated with an interconnect connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Delete Tag**.
7. **Tag Name**: From the drop-down list, choose a tag name.
8. Click **Delete**.

Create Microsoft-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Attach Megaport Template to Cisco Catalyst 8000v Instance.
6. Create Interconnect Gateways at Megaport Location.

   For connectivity to Microsoft Azure, create a pair of Interconnect Gateways in the Megaport fabric. Redundant connectivity is the default and only supported configuration.
7. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.

5. **Choose Interconnect Account**: Choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: Choose the Interconnect Gateway from which the connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Microsoft Azure**.
Azure Account	Choose a Microsoft Azure account by the account name entered while associating the account details with Cisco SD-WAN Manager.

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. Equinix ExpressRoutes are not supported in Cisco vManage Release 20.6.1 and Cisco vManage Release 20.7.1. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following and click **Save**: • Resource Group: Choose a resource group associated with the Microsoft Azure account. • Region: Choose an Azure region. • Instance Name: Enter a name for the ExpressRoute instance. • Provider: Choose **Megaport**. • Peering Location: Click the Refresh button to update the list of available locations. Choose an ExpressRoute location. • Bandwidth: Choose the bandwidth of the ExpressRoute circuit. • SKU: Choose the **Premium** or the **Standard** SKU. • Billing Model: Choose **Metered** billing or **Unlimited**.

10. Configure the following settings for the primary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.

Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

11. Configure the following settings for the secondary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	The bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which the secondary connection must be established.

12. Configure the following and click **Next**:

Deployment Type	Choose **Public**.
Primary IPv4 Subnet	Enter a /30 CIDR public IP address for BGP peering from the primary Interconnect Gateway. Before creating the connection, ensure that your organization is permitted to use the public IPv4 address.
Secondary IPv4 Subnet	Enter a /30 CIDR public IP address for BGP peering from the secondary Interconnect Gateway. Before creating the connection, ensure that your organization is permitted to use the public IPv4 address.
BGP Advertise Prefix	Enter the summary addresses and prefixes you wish to advertise to the Interconnect Gateway.
Segment	Choose a segment ID for this connection.

13. Review the connection summary.

- To create the connection, click **Save**.
- To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched. This task creates the following resources:

- virtual cross connects in the Megaport fabric between the Interconnect Gateways and the ExpressRoute
- Microsoft Azure public/private peerings for ExpressRoute circuits
- a vNet gateway, if a vNet gateway does not exist for a vNet
- connections between the ExpressRoute and the vNet gateways

When the task is successful, the connections are listed on the **Interconnect Connectivity** page.

You can also view the connection details on the Microsoft Azure portal.

Create Private-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways

Prerequisites

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag Microsoft Azure VNets.
6. Attach Megaport Template to Cisco Catalyst 8000v Instance.
7. Create Interconnect Gateways at Megaport Location.

   For connectivity to Microsoft Azure, create a pair of Interconnect Gateways in the Megaport fabric. Redundant connectivity is the default and only supported configuration.
8. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.
5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Microsoft Azure**.
Azure Account	Choose a Microsoft Azure account by the account name entered while associating the account details with Cisco SD-WAN Manager.

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. Equinix ExpressRoutes are not supported in Cisco vManage Release 20.6.1 and Cisco vManage Release 20.7.1. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following and click **Save**: • Resource Group: Choose a resource group associated with the Microsoft Azure account. • Region: Choose an Azure region. • Instance Name: Enter a name for the ExpressRoute instance. • Provider: Choose **Megaport**. • Peering Location: Click the Refresh button to update the list of available locations. Choose an ExpressRoute location. • Bandwidth: Choose the bandwidth of the ExpressRoute circuit. • SKU: Choose the **Premium** or the **Standard** SKU. • Billing Model: Choose **Metered** billing or **Unlimited**.

10. Configure the following settings for the primary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.

Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

11. Configure the following settings for the secondary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	The bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which the secondary connection must be established.

12. Configure the following and click **Next**:

Deployment Type	Choose **Private**.

BGP-Peering Settings	Choose **Auto-generated** or **Custom**.
	Auto-generated: The interconnect BGP ASN, and the primary and secondary IPv4 subnets are selected by the system. The IPv4 subnets are selected from an internally reserved /16 subnet (198.18.0.0/16).
	Custom:
	Note
	You can specify a custom BGP ASN and custom IPv4 subnets only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.
	• **BGP ASN**: Specify an ASN of your choice for the primary and secondary peering with the ExpressRoute.
	• **Primary IPv4 Subnet**: Enter a /30 CIDR IP address for BGP peering with the primary Interconnect Gateway.
	• **Secondary IPv4 Subnet**: Enter a /30 CIDR IP address for BGP peering with the secondary Interconnect Gateway.
	• Beginning with Cisco vManage Release 20.8.1:
	  • The custom subnet IP addresses must be in the following range: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.
	  • The custom subnet must be specified as /30.
	  • The custom subnet should not conflict with 172.31.251.0/21.
	  • The custom subnet must not conflict with the subnets used for other connections.

Attachment	Choose one of the following: • **vNet**: Attach VNets to the connection using VNet tags. • **vWAN**: Attach virtual WAN to the connection and choose VNets from the regions of the virtual WAN using VNet tags. • Minimum supported release: Cisco vManage Release 20.9.1 **Cloud Gateway**: Attach cloud gateways to the connection. You can select upto 5 cloud gateways per connection.
VNet Settings	**VNet Tags**: Choose VNet tags to identify VNets for which traffic must be routed through this connection.

virtual WAN Settings	**vWAN**: Choose or add a new virtual WAN. **Note** You can choose the virtual WAN to be attached only for the first connection to Microsoft Azure from an interconnect gateway. The same virtual WAN is attached to any subsequent connection to which you choose to attach a virtual WAN. Starting from Cisco vManage Release 20.8.1, Cisco SD-WAN Manager supports one vWAN per Microsoft Azure resource group per Microsoft Azure account. Once that vWAN is chosen and used as part of a vWAN connection, subsequent vWAN connections to the same Microsoft Azure resource group use the same vWan. The Microsoft Azure resource group is determined for the connection when the Express Route Circuit is selected for it. All other Microsoft Azure resources belonging to the connection must be in the same Microsoft Azure resource group as that of the selected Express Route Circuit. **vNet**: Choose VNet tags to identify VNets for which traffic must be routed through this connection. Cisco SD-WAN Manager finds VNets based on the chosen VNet Tags, and identifies the regions to which the VNets belong. For the chosen virtual WAN and the identified regions, Cisco SD-WAN Manager finds and lists the available virtual hubs for verification. For regions where a virtual hub does not exist, you must specify the name and address-prefix to add a virtual hub. **vHub Settings**: **Note** From Cisco Catalyst SD-WAN Manager Release 20.12.1, if multiple Azure Virtual WAN hubs are there in a region, you can select a particular Azure Virtual WAN hub for that region. Once you choose the Azure Virtual WAN hub, all subsequent connections created for Azure Virtual WAN uses the same Azure Virtual WAN hub. **a.** Click **Add Settings**. Or, if you're modifying the configuration, click **Edit Settings**. **b.** Review the virtual hub name and address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.
Segment	Choose a segment ID for this connection.

13. Review the connection summary.

- To create the connection, click **Save**.
- To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched.

For VNet attachmment, the configuration task creates the following resources:

- virtual cross connects in the Megaport fabric between the Interconnect Gateways and the ExpressRoute
- Microsoft Azure public/private peerings for the ExpressRoute circuits
- a vNet gateway, if a vNet gateway does not exist for a vNet
- connections between the ExpressRoute and the vNet gateways

For virtual WAN attachment, the configuration task creates the following resources:

- virtual cross connects in the Megaport fabric between the Interconnect Gateways and the ExpressRoute
- Microsoft Azure public/private peerings for the ExpressRoute circuits
- necessary virtual hubs
- connections between vNets and virtual hubs
- an ExpressRoute Gateway for each virtual hub, if necessary
- connections between the ExpressRoute Gateway and ExpressRouteCircuits

When the task is successful, the connections are listed on the **Interconnect Connectivity** page.

You can also view the connection details on the Microsoft Azure portal.

Create Interconnect Between Interconnect Gateways

In Cisco SD-WAN Manager, you can create an interconnect between Interconnect Gateways at two or more Megaport locations. By doing so, you can link the Cisco Catalyst SD-WAN branch locations connected to these Interconnect Gateways via the Megaport fabric.

Prerequisites

For each Cisco Catalyst SD-WAN branch location to be connected through the Megaport fabric,

1. Associate Megaport Account with Cisco SD-WAN Manager.
2. Configure Global Settings for Interconnect Gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Identify the nearest Megaport location.
5. Create an Interconnect Gateway at the Megaport location closest to the branch location.

Note If you have a VRF defined in two branch locations and wish to exchange traffic attached to the VRF through the connection between the Interconnect Gateways, you must configure the VRF and an appropriate Centralized Policy on the Interconnect Gateways to route the branch traffic through the connection between the Interconnect Gateways.

6. From Cisco vManage Release 20.9.1, ensure that you have the required license to create the connection. Without the required license, connection creation fails. For more information, see License Management for Cisco SD-WAN Cloud Interconnect with Megaport.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **MEGAPORT**.

Note This field is introduced in Cisco vManage Release 20.6.1.

5. **Choose Interconnect Account**: choose a Megaport account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the source Interconnect Gateway.
7. (Minimum release: Cisco vManage Release 20.9.1) To view available Interconnect Connection licenses associated with the Megaport account, click **Check available licenses**.
8. Click **Add Connection**.
9. Configure the following and click **Next**:

Destination Type	Choose **Edge**.
Provider	Choose **Megaport**. **Note** This field is not available from Cisco vManage Release 20.6.1.
Connection Name	Enter a unique name for the connection.
Interconnect Gateway	Choose destination Interconnect Gateway.
Bandwidth	Specify the connection bandwidth. Unit: Mbps.

10. Review the connection summary.
    - To create the connection, click **Save**.

- To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Verify and Modify Configuration

View Interconnect Gateway and Connection Summary

On the **Interconnect** page, you can view a summary of Interconnect Gateways and connections that you have created. If you have not created any Interconnect Gateways, the page provides an overview of the workflow for creating and managing Interconnect Gateways and connections.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.

   The following information is displayed:

Interconnect Gateways	• Total number of Interconnect Gateways • Number of Interconnect Gateways that reachable (Up) • Number of Interconnect Gateways that are unreachable (Down)
Connections	• Total number of connections • Number of connections in the Up state • Number of connections in the Down state
Summary Table	Summarized list of all Interconnect Gateways and connections from the gateways.

View, Edit, or Delete Connections

View Connection Properties

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

   Existing connections are summarized in a table.
4. To view more information about a connection, click **...** for the desired connection and click **View**.

Edit Connection Configuration

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

   Existing connections are summarized in a table.
4. To modify connection configuration, click **...** for the desired connection and click **Edit**.

   The following tables describe the editable parameters based on connection destination and connection type, if any. Configure the parameters as required.

   Along with these editable parameters, Cisco SD-WAN Manager also displays read-only properties about the connection.

Note You can modify the properties of active connections only.

Table 82: Editable Properties of Interconnect Connections to AWS

Field	Description	Applicable Connection Types
Bandwidth	Modify the connection bandwidth. Unit: Mbps.	Private and Public Hosted VIF
Segment	Minimum supported release: Cisco vManage Release 20.10.1 Choose a different segment ID for this connection.	All connections to AWS

Field	Description	Applicable Connection Types

Transit Gateway	Minimum supported release: Cisco vManage Release 20.10.1
	a. Click the Refresh button to fetch the transit gateways associated with the selected AWS account.
	b. Choose the transit gateway to which the Direct Connect connection must be created.
	Note
	• You can remove a transit gateway subject to the following conditions:
	  • The transit gateway that you wish to remove is not the only transit gateway associated with the connection.
	  • You remove VPC tags corresponding to the region served by the transit gateway in the same edit operation.
	• You cannot replace an existing transit gateway for a region with another transit gateway from the same region.
		Transit Hosted Connections

VPC Tags	Minimum supported release: Cisco vManage Release 20.10.1 Choose VPC tags to identify VPCs for which traffic must be routed through this connection.	• Private Hosted VIF and Private Hosted Connections with VPC attachments • Transit Hosted Connections
Allowed Prefixes	Minimum supported release: Cisco vManage Release 20.10.1 Click **Edit Prefixes**. Enter the IPv4 CIDR prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard. **Note** You can only add more prefixes. You cannot remove existing prefixes.	Transit Hosted Connections

Table 83: Editable Properties of Interconnect Connections to Google Cloud

Field	Description
Connection Speed	Choose the desired bandwidth from the **Connectivity Speed** drop-down list. In the case of redundant connnections, modify the connection speed of either the primary or the secondary connection. The peer connection is updated to use the same connection speed. The bandwidth options for a connection may depend on the associated peering location.

Note
Modify the property of either the primary or the secondary connection. The peer connection is updated to use the same configuration.

Table 84: Editable Properties of Interconnect Connections to Microsoft Azure

Field	Description	Applicable Connection Types
Bandwidth	Modify the connection bandwidth. Unit: Mbps. **Note** You can only increase the bandwidth of connections to Microsoft Azure. For connections to Microsoft Azure, you must increase the bandwidth of the ExpressRoute on the Azure portal before increase the connection bandwidth on Cisco SD-WAN Manager.	Private and Public (Microsoft) Peering Connections
Segment	Minimum supported release: Cisco vManage Release 20.10.1 Choose a different segment ID for this connection.	Private and Public (Microsoft) Peering Connections
BGP Advertise Prefix	Minimum supported release: Cisco vManage Release 20.10.1 Enter the summary addresses and prefixes you wish to advertise to the Interconnect Gateway. **Note** By default Microsoft Azure uses an older version of API on its portal for displaying resources or network objects that do not display the BGP advertise prefix correctly. To verify the BGP advertise prefix from the Microsoft Azure portal, select 2020-05-01 or above API version.	Public (Microsoft) Peering Connections
vNet Settings		

Field	Description	Applicable Connection Types
vNet	Minimum supported release: Cisco vManage Release 20.10.1 Choose VNet tags to identify the VNets for which traffic must be routed through this connection.	Private Peering Connections
vHub Settings	Minimum supported release: Cisco vManage Release 20.10.1 **a.** Click **Edit Settings**. **b.** Review the virtual hub name and address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.	Private Peering Connections

Table 85: Editable Properties of Interconnect Connections Between Edge Devices

Field	Description
Bandwidth	Modify the connection bandwidth. Unit: Mbps.

5. To apply the changes, click **Update** or **Save**.

Delete Connection

Note

- When you delete a connection to AWS, Cisco SD-WAN Manager deletes only the VIF, the virtual private gateway, and the route table that were created while establishing the connection.
- While creating a connection to AWS, if you created a direct connect gateway or a transit gateway, from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can optionally delete the direct connect gateway and transit gateway.
- When you delete a connection to Microsoft Azure, Cisco SD-WAN Manager deletes any ExpressRoutes, VNet gateways, ExpressRoute gateways, and virtual hubs created for the connection only if these elements are not used in other connections.

  From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can optionally choose to delete Express-Route and Virtual Wan at the time of deleting a connection, or manage these Azure resources as required. When you delete a GCP connection, you can optionally select to delete the Google Cloud Router, or manage these resources as required.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

   Existing connections are summarized in a table.
4. To delete a connection, click **...** for the desired connection and click **Delete**. Confirm that you wish to delete the connection.

View, Edit, or Delete an Interconnect Gateway

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Gateway Management**.

   Existing Interconnect Gateway details are summarized in a table.
4. In the table, click **…** for the desired Interconnect Gateway.
   - To view more information about the Interconnect Gateway, click **View**.
   - To edit the Interconnect Gateway description, click **Edit Interconnect Gateway**.
   - To delete the Interconnect Gateway, click **Delete** and confirm that you wish to delete the gateway.

Note You can delete an Interconnect Gateway only if there are no connections associated with it.

Deleting the Interconnect Gateway disconnects the branch location from the Megaport fabric.

View, Edit, or Delete an Interconnect Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Account Management**.

   The available interconnect accounts are listed in a table.
4. In the table, click **...** for the desired interconnect account.

   - To view more details about the interconnect account, click **View**.
   - To modify interconnect account details, click **Edit Account Information**.

     You can modify the **Account Name** and the **Description**.
   - To modify interconnect account credentials, click **Edit Account Credentials**.

     You can modify the **User Name** and **Password** for the account.

Note Modifying the credentials on Cisco SD-WAN Manager, does not modify the credentials with the Interconnect Provider. Use this configuration option only to replicate any changes to the account credentials that you have performed on the relevant portal of the Interconnect Provider.

   - To delete the interconnect account, click **Remove** and confirm that you wish to remove the account.

Audit Management

The fabric of the SDCI provider, Megaport, incorporates audit management support that assists you in verifying the synchronization of the cloud connection state with the Cisco SD-WAN Manager state. The audit process scans the provider resources, interconnect gateways, and connections to the cloud. In the **Audit** screen, when there are errors, they are displayed and if there are no errors, the status is displayed as **In Sync**.

Note In the Cisco vManage Release 20.11.1, the audit management feature is supported only on the Megaport fabric.

Accessing the Audit Report

1. In **Cloud OnRamp for Multicloud**, navigate to the **Interconnect** tab.
2. In the **Intent Management** pane, click **Audit**.
3. In **Intent Management- Audit**, under **Interconnect Gateways**, choose an **Interconnect Provider** from the drop-down list.

4. Choose a **Destination Type** and choose a **Cloud Provider** from the drop-down list when the Destination Type is **cloud** to view the desired audit report.

Note Choose **Destination Type** as **cloud** or **edge** depending on the requirement.

Note The following are the different connections that are scanned and reported by the audit report:

- **Edge Gateway** indicates that there are edge gatways created using Cisco SD-WAN Manager workflows with the respective details.
- **Edge Connections** indicates that there are edge connections created using Cisco SD-WAN Manager workflows with the respective details.
- **Unknown Edge Gateways** indicates that Cisco SD-WAN Manager is unable to recognize certain edge gateways.
- **Unknown Edge Connections** indicates that Cisco SD-WAN Manager is unable to recognize certain edge connections.

The following are the statuses that are displayed in the audit report:

- **In Sync**
- **Out of Sync**
- **AUDIT_INFO**

Benefits of Audit

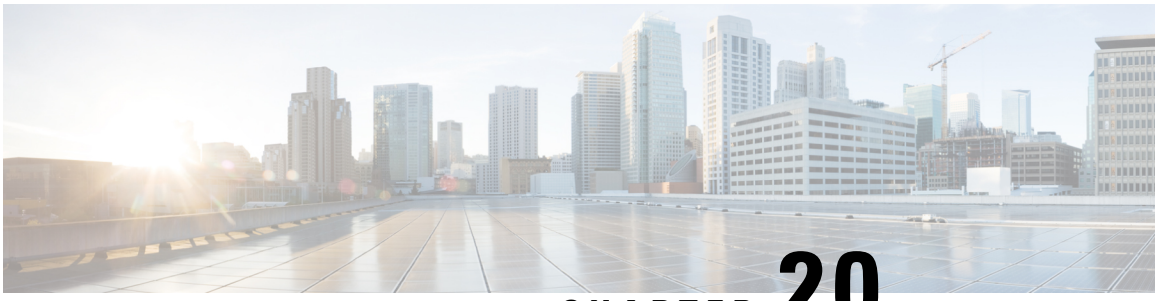
Audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what has been realized in the cloud. The gaps are in terms of cloud resources, connectivity and states. When such gaps are detected, Cisco SD-WAN Manager flags such gaps and helps you take corrective action.

Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Megaport

Scenario	Resolution
Unable to add Interconnect Account	• Verify that the account credentials associated with Cisco SD-WAN Manager are correct. • If you updated the credentials with Interconnect Provider, update the account credentials on Cisco SD-WAN Manager.

Scenario	Resolution
While attempting to create an Interconnect Gateway, the device list is empty	Verify that the devices has been assigned a template. (Recommended template: *Default_MEGAPORT_ICGW_C8000V_Template_V01*)
While attempting to create an Interconnect Gateway, cannot find the desired location	Click the Refresh button to update the list of available locations.
Creation of Interconnect Gateway failed	**1.** Check the configuration task progress on Cisco SD-WAN Manager for any error messages. **2.** If you are using the Interconnect Global Settings, check whether the selected software image is available at the Interconnect Provider location. **3.** If the VM instance is not deployed or the IP pool is exhausted, check with the Interconnect provider.
While creating a Direct Connect connection, the Direct Connect gateway or the transit gateway list is empty	**1.** On the AWS portal, verify that the desired Direct Connect gateway or transit gateway is available. **2.** Click the Refresh button to fetch the list of gateways from AWS. **3.** If a gateway is not available in AWS, create the gateway through Cisco SD-WAN Manager.
While creating a Direct Connect connection, host VPC tags are not listed	Verify that the host VPC tags are available and enabled for Interconnect Connectivity.
Creation of Direct Connect connection failed	**1.** Check the configuration task progress on Cisco SD-WAN Manager for any error messages. **2.** If you are using the Interconnect Global Settings, check whether the internal IP address pool has been exhausted. If yes, delete some connections and retry. **3.** If you are using custom settings, ensure that you haven't entered overlapping CIDR subnets for peering. **4.** Check whether you have reached any connection limits. See *Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Megaport*. **5.** Verify permissions of the Interconnect Provider account and the AWS account.

Scenario	Resolution
Traffic flow issues	1. Ensure that the required security rules for inbound and outbound traffic are configured for the host VPC. 2. Verify whether the virtual interface has been created and attached to the Direct Connect gateway. 3. In AWS, verify whether the BGP peering status is in the UP state for the virtual interface. 4. Verify whether the correct route table is being used as the main routing table for the host VPC and whether the necessary routes are being propagated towards the virtual private gateway or the transit gateway. 5. Verify whether the virtual private gateway or transit gateway is attached to the Direct Connect gateway.
Latency issues	1. Verify whether the Interconnect Gateway location is in close proximity to the Direct Connect location chosen while creating the connection. 2. Ensure that you have configured the appropriate bandwidth for the connection.
Cloud Gateways are not displayed in the drop-down list	Ensure that the necessary Cloud Gateways are created using the Multicloud workflow and the minimum requirements listed in this document are met.
Traffic to VPC or VNET workload is sent over the internet even after creating an Interconnect Connection to the Cloud Gateway	When an Cisco Catalyst SD-WAN branch is connected to a Cloud Gateway through the internet and through an Interconnect Connection from an Interconnect Gateway to access the same VPC or VNET workload, by default, traffic from the branch is sent through the internet. To make the private path through the Interconnect Gateway the preferred path, apply appropriate control and data policies to the WAN edge device at the branch, the Interconnect Gateway, and the Cloud Gateway.



CHAPTER 20

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Table 86: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy a Cisco Cloud Services Router 1000v (Cisco CSR 1000v) instance as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway. From the Interconnect Gateway, you can create software-defined interconnects to an AWS Cloud OnRamp or another interconnect gateway in the Equinix fabric.
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix: Google Cloud and Microsoft Azure	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can create software-defined interconnects to Google Cloud VPCs, or Microsoft Azure VNets or Virtual WANs to link your branch location to the cloud resources through the Equinix fabric. You can also create, update and delete device links from Interconnect Gateway in the Equinix fabric.

Feature Name	Release Information	Description
Encrypted Multicloud Interconnects with Equinix	Cisco vManage Release 20.9.1	You can extend the Cisco Catalyst SD-WAN fabric from the Interconnect gateway in Equinix into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers. You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager.
Support for Cisco Catalyst 8000V Edge Software	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can deploy a Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway.
Addition of VPC and VNet Tags to SDCI Connections	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can modify VPC and VNet Tags and some other properties that are associated with an SDCI connection
Management of Audit in Equinix	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	The audit management helps in understanding if the interconnect cloud and provider states are in sync with the Cisco Catalyst SD-WAN Manager state. The audit process involves scanning the provider resources, interconnect gateways, and connections to the cloud. For more information, see Audit Management.

- Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 499
- Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 499
- Information About Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 505
- Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 508
- Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Equinix, on page 510
- Create Interconnect to AWS, on page 515
- Create Interconnects to Google Cloud, on page 524
- Create Interconnects to Microsoft Azure, on page 533
- Device Links, on page 545
- Create Interconnect Between Interconnect Gateways, on page 547

- Verify and Modify Configuration for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 549
- Audit Management, on page 554
- Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Equinix, on page 556

Prerequisites for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.

   After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* documentation in the Equinix Developer Platform Knowledge Center.

   Create billing accounts for each region in which you would like to deploy an Interconnect Gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.

2. For a connection that requires a public peering between an Interconnect Gateway and a Cloud provider, specify a public BGP peering IP address. Ensure that your organization is permitted to use the public IP address before you create the connection. Alternatively, you can allocate the public IP address for BGP peering from the Equinix portal.

3. Ensure you have UUIDs for the required number of Cisco CSR 1000v instances that you wish to deploy as Interconnect Gateways.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy Cisco Catalyst 8000v instance.

4. Ensure that Cisco SD-WAN Manager can connect to the Internet.

   As part of the configuration workflows, Cisco SD-WAN Manager connects to the Equinix portal via the Internet.

5. The Cisco SD-WAN Manager certificate must be signed by Cisco (Automated) PKI or Symantec as the root CA for Cisco SD-WAN Manager to be able interact with Equinix. We recommend using a Cisco (Automated) PKI certificate. Enterprise CA certificate is supported starting Cisco vManage Release 20.9.1.

6. For existing Cisco CSR 1000V deployments: Upgrade Cisco SD-WAN Manager to Release 20.9.5 or later, then upgrade the Cisco CSR 1000V to Cisco Catalyst 8000V to continue using Cisco virtual devices as the Interconnect Gateway in the Equinix Fabric.

   For more information, see Cisco SD-WAN Manager Upgrade Paths.

Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

General

- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can create and edit the connections.

Prior to Cisco Catalyst SD-WAN Manager Release 20.12.1, you cannot edit the connections. You can delete the connection and create a new connection with the desired settings.

- Interconnect gateways in the same location cannot be created or deleted at the same time.
- All interconnect and cloud operations are time bound. If an operation times out, Cisco SD-WAN Manager reports a failure. Currently, the time out values are not configurable.
- If you modify the global settings, the changes are applied to any new gateways or connections created after the modification. The changes do not affect gateways or connections created before the modification.
- If you have deployed Equinix Interconnect Gateway in Cisco IOS XE Catalyst SD-WAN Release 17.3.3 through Cisco SD-WAN Manager prior to Cisco Catalyst SD-WAN Manager Release 20.12.1, you must upgrade the Equinix Interconnect Gateway to Cisco IOS XE Catalyst SD-WAN Release 17.9.x before you upgrade Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.12.1.
- After you create an interconnect gateway at an Equinix location using Cisco vManage Release 20.6.1, if you upgrade Cisco SD-WAN Manager software to a later release, port 443 on the interconnect gateway is disabled. To overcome this limitation, do one of the following:
  - Enable port 443 manually.
  - Delete the existing interconnect gateway and create a new interconnect gateway after the Cisco SD-WAN Manager software upgrade.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.2, any transit gateway created as part of the multicloud workflow is not listed under the transit connections of SDCI workflow.
- Starting from Cisco vManage Release 20.9.5, you can deploy Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric.

Interconnects to AWS

- While creating a connection to an AWS cloud resource, be mindful of the AWS quotas and limitations. Cisco SD-WAN Manager does not enforce all the AWS quotas and limitations.
- You cannot use cloud resources belonging to different AWS accounts as part of a single connection.
- Equinix only supports public, private, and transit VIFs over a hosted connection. Hosted VIFs are not supported.
- Attach either private VIFs or transit VIFs to a Direct Connect gateway. You cannot attach a combination of private VIFs and transit VIFs to the same Direct Connect gateway.
- From Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, for a transit-hosted connection, in an AWS region, you can associate only one transit gateway with a Direct Connect gateway.

  We recommend that you associate only one transit gateway with a direct connect gateway in an AWS region with Cisco vManage Release 20.9.1 and earlier releases.
- When editing interconnect transit connection, if a new transit gateway is selected without a VPC tag in the same region, connection update is discarded.
- All connections to a particular VPC must
  - peer with the same direct connect gateway
  - have the same transit gateway or virtual private gateway attachment

- For a transit VIF, the transit gateway and direct connect gateway must use different BGP ASNs.
- While creating host VPC tags, choose to use the tag with either the AWS Multi Cloud workflow or the interconnect connectivity workflow. This choice cannot be altered after the tag is created and persists till the deletion of the tag.
- A host VPC tag selected for interconnect connectivity cannot be edited after creation.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can create and edit the host VPC tag.

Interconnects to Microsoft Azure

- While creating host VNet tags, choose to use the tag with either the Microsoft Azure Multicloud workflow or the interconnect connectivity workflow. This choice cannot be altered after the tag is created and persists till the deletion of the tag.
- A host VNet tag selected for interconnect connectivity cannot be edited after creation.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can create and edit the host VNet tags.
- While creating a private-peering connection to a Microsoft Azure ExpressRoute from an interconnect gateway, you can attach to the connection only the VNets, virtual WANs, and virtual hubs that belong to the same resource group as the ExpressRoute circuit. Attaching VNets, virtual WANs, and virtual hubs from a different resource group is not a supported configuration.

Interconnects to Google Cloud

- Each Cloud Router must use the same ASN for all its BGP sessions.

Device Links

- The fixed Bandwidth for all links in a device group can range from 50 Mbps to 10 Gbps.
- The cumulative bandwidth of all links at a given metro should not be greater than 10 Gbps.

Restrictions for Encrypted Multicloud Interconnects

Minimum supported release: Cisco vManage Release 20.9.1

Interconnects to AWS

- As per AWS requirement,
  - The minimum instance type must be x-large for Cloud Gateways.
  - A maximum of 10 Cloud Gateways can be attached to a single interconnect connection.
  - One Cloud Gateway can be connected to 30 interconnect connections.

Interconnects to Microsoft Azure

- A single Cloud Gateway can be attached to 8 different cloud interconnect connections and one interconnect connection can connect to 5 different Cloud Gateways.
- To connect to Cloud Gateways in different regions, the express route circuit must be of Premium type.
- For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the Cloud Gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, Interconnect Gateway and Cloud Gateway.

Interconnects to Google Cloud

- Cloud Interconnect connection to Google Cloud Gateway is supported only with redundancy enabled.
- Only one Google Cloud Gateway can be attached to a single connection.
- Existing Google Cloud Gateways are not supported for cloud interconnects.
- A maximum of 5 Google Cloud Routers can be created for a combination of region and network.

Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Table 87: Connection Configuration Limits

Description	Count
Interconnect Gateway	
Maximum number of connections (VXC) per Interconnect Gateway	20 **Note**: Aggregate VXC bandwidth should not exceed the bandwidth capacity of the Interconnect Gateway.
Interconnects to AWS	
Maximum number of VPCs per connection to AWS for a private VIF	10
Number of VPCs per connection to AWS for a transit VIF	Default: 15 Maximum: 15000
Maximum number of transit gateways per connection to AWS for a transit VIF	3
Maximum number of Direct Connect gateways per connection	1
Maximum number of VIFs (private or transit) per AWS Direct Connect gateway	Default: 30 Limit can be increased on request.

Description	Count
Maximum number private, public, or transit VIFs per AWS Direct Connect hosted connection	1
Maximum number of prefixes from branch location to AWS for a transit VIF	100
Maximum number of prefixes per AWS transit gateway from AWS to a branch location for a transit VIF	20
Interconnects to Microsoft Azure	
Maximum number of Interconnect Gateways that can connect to an ExpressRoute	2
Maximum number of VNets to which an ExpressRoute can connect	10
Maximum number of ExpressRoutes that can connect to a VNet	4
Maximum number of ExpressRoutes that can connect to a virtual hub	8 per peering location
Maximum aggregate throughput per virtual WAN ExpressRoute gateway	20 Gbps
Maximum number of VNets that can connect to a virtual hub	500 - (total number of virtual hubs in the virtual WAN)

Interconnects to AWS

- When you delete a private VIF connection to AWS, Cisco SD-WAN Manager deletes the VIF, the virtual private gateway, and the route table that were created while establishing the connection.
- When you delete a transit VIF connection, Cisco SD-WAN Manager removes any attachments and associations to a Direct Connect gateway, transit gateway, or virtual private gateway that were created while establishing the connection.
- While creating a connection to AWS, if you created a direct connect gateway or transit gateway from Cisco SD-WAN Manager, deleting the connection does not delete the gateway. You need to manage these AWS resources as required.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you have the option to delete the Direct Connect Gateway or Transit Gateway while deleting the connection.
- When you create a connection, a new route table is created and set as the Main route table for the host VPCs attached to the connection. A default route is created in the Main route table to the transit gateway and route propagation is enabled. Edit the routes and propagation as required.

  From Cisco vManage Release 20.5.1, the static routes and subnet associations required to be accessed by the interconnect should be moved to the newly created main route table by Cisco SD-WAN Manager.

Interconnects to Google Cloud

- For nonredundant connectivity, you must deploy a Google Cloud Router in each network-region and create a VLAN attachment for each Google Cloud Router.
- For redundant connectivity, you must deploy two Google Cloud Routers in each network-region and create a VLAN attachment for each Google Cloud Router.
- For use with interconnect attachments, you must set the Google ASN for the Google Cloud Routers to 16550.

Interconnects to Microsoft Azure

- Only one pair of Interconnect Gateways can connect to a particular ExpressRoute to provide a HA connection to the VNet attched to the ExpressRoute.

  To connect a second pair of Interconnect Gateways to the same vNet, do as follows: create another ExpressRoute; attach the vNet to the ExpressRoute; and connect the Interconnect Gateways to the ExpressRoute

  You can have a maximum four such ExpressRoutes connecting to a VNet, and connect each Express Route to a pair of Interconnect Gateways.

- An ExpressRoute can connect to maximum of 10 VNets. You can attach VNets to an ExpressRoute while creating connections to the ExpressRoute from Interconnect Gateways. VNets are attached based on the VNet tags you choose for the connection.

  If you choose a VNet tag that applies to more than 10 VNets or choose a combination of VNet tags so that the total number of select VNets is more than 10, interconnect creation fails.



Note Any VNets that you may have attached to the ExpressRoute from the Azure portal are also considered while determining the number VNets that you can attach to the ExpressRoute while creating the connection from the interconnect gateways.

- In the Azure portal, if cloud gateway extension connections intended for one ExpressRoute gateway also appear in a second ExpressRoute gateway, create two ExpressRoute gateways with a different prefix.
- You can connect a VNet to either a VNet gateway or an ExpressRoute gateway. So, if you have created a private peering to a VNet through a VNet gateway, you cannot create a private peering to the same VNet through an ExpressRoute gateway, and vice-versa.
- If a VNet is connected to virtual hub in a virtual WAN, the same VNet cannot be connected to another virtual WAN.
- All the VNets in a region must connect to a single virtual hub in the same region.
- Redundant connectivity is the default and only supported configuration. You must create connections to Microsoft Azure from a pair of Interconnect Gateways in the Equinix fabric.

  When choosing a pair of Interconnect Gateways from which you wish to create the primary and secondary connections to a Microsoft Azure ExpressRoute, ensure that the Interconnect Gateways are configured to use the same BGP ASN for BGP peering.

Information About Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

From Cisco SD-WAN Manager, you can deploy a Cisco Cloud Services Router 1000v (Cisco CSR 1000v) instance in the fabric of the SDCI provider Equinix and add the instance as a WAN edge device in the Cisco SD-WAN fabric. As a WAN edge device, the Cisco CSR 1000v instance links a branch location to the Equinix fabric. In the Equinix fabric, the Cisco CSR 1000v instance acts as an interconnect gateway. From the interconnect gateway, you can create a direct Layer 2 connection (an interconnect) in the Equinix fabric to a Cloud OnRamp or another interconnect gateway. The interconnects link branch locations, or link branch locations to cloud service providers through the interconnect gateways in the Equinix fabric.

In this setup, the Cisco SD-WAN fabric acts as the overlay network, and the Equinix fabric acts as the underlay network. The Equinix fabric provides efficient, high-speed, low-latency, high-bandwidth connectivity to cloud resources in multiple global locations. We recommend that you deploy the Cisco CSR 1000v instance at an Equinix location closest to your branch location.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy Cisco Catalyst 8000v instance.

You can create the following types of connections from an interconnect gateway:

Table 88: Connection Types

Destination	Connection Types	Supported Software Releases
Amazon Web Services	• Direct-connect-private-hosted connection to AWS direct-connect-gateway from interconnect gateway • Direct-connect-public-hosted connection to AWS from interconnect gateway • Direct-connect-transit-hosted connection to AWS direct connect gateway from interconnect gateway	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Catalyst SD-WAN Release 17.3.3
Microsoft Azure	• Partner ExpressRoute Circuit - Microsoft Peering • Partner ExpressRoute Circuit - Private Peering	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Catalyst SD-WAN Release 17.3.3

Destination	Connection Types	Supported Software Releases
Google Cloud	Partner Interconnect Attachment to a Google Cloud Router	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Release 17.3.3
Interconnect Gateway	Link between Cisco Catalyst SD-WAN branch locations connected to the interconnect gateways	Cisco Catalyst 8000v with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco CSR 1000v with Cisco IOS XE Catalyst SD-WAN Release 17.3.3.

Cisco Catalyst SD-WAN Manager serves as a unified management portal and enables you to perform the following tasks:

- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, configure Cisco Catalyst 8000v instance.

  Configure and deploy the Cisco CSR 1000v instance at an Equinix location for prior to Cisco Catalyst SD-WAN Manager Release 20.12.1.

- Create cloud interconnects to public cloud resources.
- Create interconnects to link Cisco Catalyst SD-WAN branch locations through the Equinix fabric.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy a Cisco Catalyst 8000v instance as the interconnect gateway in the Equinix fabric and connect anCisco Catalyst SD-WAN branch location to the interconnect gateway. Existing Cisco CSR1000V deployments can be used to create connections.

Points to Consider

If you are upgrading from an earlier Cisco Catalyst SD-WAN Manager version to Cisco Catalyst SD-WAN Manager Release 20.12.1, to enable Cisco Catalyst 8000v:

- Re-authenticate the existing Equinix account through **Edit Account Credentials** and provide the customer key and the customer secret. You can use the same key and the secret that you used for previous versions. It internally updates the billing accounts and locations available for Cisco Catalyst 8000v. For information on editing account details, see View, Edit, or Delete an Interconnect Account.
- After the account is re-authenticated, you must update the **Global Settings** for interconnect gateways to select the Cisco Catalyst 8000v software version and other parameters for new gateways. For information on updating global settings, see Configure Global Settings for Equinix Interconnect Gateways.

- If you have deployed Equinix interconnect gateway using Cisco IOS XE Catalyst SD-WAN Release 17.3.3 via Cisco SD-WAN Manager prior to Cisco Catalyst SD-WAN Manager Release 20.12.1, the Equinix interconnect gateway must be upgraded from Cisco IOS XE Catalyst SD-WAN Release 17.3.3 to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or Cisco IOS XE Catalyst SD-WAN Release 17.9.1a before upgrading to Cisco Catalyst SD-WAN Manager Release 20.12.1.

Benefits of Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

1. Branch locations connect seamlessly to the Equinix fabric over the Cisco Catalyst SD-WAN fabric.
2. Interconnects to public cloud with assured SLAs.
3. End-to-end traffic security, segmentation, and policy through the Cisco Catalyst SD-WAN fabric.
4. Cisco SD-WAN Manager provides a single pane to manage your connectivity to any cloud.
5. End-to-end visibility across the Cisco Catalyst SD-WAN and Equinix fabric.
6. Links between Cisco Catalyst SD-WAN branch locations and between Cisco Catalyst SD-WAN branch locations and a public cloud.

Encrypted Multicloud Interconnects

Minimum supported release: Cisco vManage Release 20.9.1

You can provision a secure private Cisco Catalyst SD-WAN connection between an Interconnect Gateway and Cloud Service Providers through the Cloud OnRamp workflows in Cisco SD-WAN Manager. You can terminate the virtual cross connects from the Interconnect Gateway in the cloud interconnect provider to the existing Cloud Gateways which are created as part of the Multicloud workflow. For more information, see Cloud OnRamp for Multicloud, on page 305. This feature enables support for both internet and private paths to access VPC and VNET workloads.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, encrypted multicloud interconnects supports AWS Cloud Gateway using Cloud WAN solution.

Benefits

- Provides end to end encryption from branch sites to Cloud Gateways through the cloud interconnect provider backbone.
- Supports multiple VPN segments over single virtual cross connect.
- Supports modification of VPC and VNET tags before and after the connection creation. VPN to VPC or VNET tag mapping can be performed using the Multicloud Intent Management screen.
- Route advertisements are controlled by Interconnect Gateways and Cloud Gateways to overcome prefix advertisements restrictions imposed by cloud service providers.

Configuration Workflow for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Prerequisite Configuration

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.

   After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* documentation in the Equinix Developer Platform Knowledge Center.

   Also, create billing accounts for each region in which you would like to deploy an interconnect gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.

2. Associate Equinix account with Cisco SD-WAN Manager.
3. Configure global settings for interconnect gateways.
4. Create necessary network segments (see Segmentation Configuration Guide).
5. Ensure you have UUIDs for the required number of Cisco CSR 1000v instances that you wish to deploy as Interconnect Gateways.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, deploy Cisco Catalyst 8000v instance.

6. Attach Equinix Template to a Cisco CSR 1000v instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can attach Cisco Catalyst 8000v instance.

7. Create interconnect gateway at Equinix location closest to your Cisco Catalyst SD-WAN branch location.

   For connectivity to Cloud Providers, create an interconnect gateway at the Equinix location.

   For connectivity between Cisco Catalyst SD-WAN branch locations, for each branch location, create an interconnect gateway at the closest Equinix location.

Workflow to Create Interconnect to AWS

Before you perform the following configuration procedures, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Associate AWS account with Cisco SD-WAN Manager.
2. Discover Host Private Networks to connect to AWS Virtual Private Clouds (VPCs).
3. Create one of the following types of connection:

Connection Type	Tip
Direct Connect - Public Hosted Connection	Use this connection for a link to a public AWS resource, with the link having a fixed bandwidth up to 10 Gbps.
Direct Connect - Private Hosted Connection	Use this connection for a dedicated link to AWS VPCs, with a link bandwidth up to 10 Gbps.

Connection Type	Tip
Direct Connect - Transit Hosted Connection	Use this connection for dedicated links up to 5,000 AWS VPCs via a transit gateway, with a link bandwidth up to 10 Gbps. You can attach up to three transit gateways to a direct connect gateway and connect to up to 15,000 VPCs.

Workflow to Link Cisco Catalyst SD-WAN Branch Locations

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

- Create an Interconnect between the interconnect gateways.

Workflow to Create Interconnect to Google Cloud

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Create the required VPC network using the Google Cloud portal.
2. Deploy Google Cloud Routers in network-regions to which you wish to connect.

   For nonredundant connectivity, using the Google Cloud portal, deploy a Google Cloud Router in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   For redundant connectivity, using the Google Cloud portal, deploy two Google Cloud Routers in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

   Starting from Cisco vManage Release 20.9.1, you can deploy Google Cloud Routers and VLAN attachments via Cisco SD-WAN Manager interconnect workflow.
3. Associate Google Cloud account with Cisco SD-WAN Manager.
4. Create Interconnects to Google Cloud Routers from interconnect gateways.

Workflow to Create Interconnect to Microsoft Azure

Before you perform the following configuration procedure, ensure that the prerequisite conditions are met and the prerequisite configuration is applied.

1. Associate Microsoft Azure account with Cisco SD-WAN Manager.
2. Discover Host Private Networks to connect to Azure Virtual Networks (VNets).
3. Create one of the following types of connection:
   - Public Peering Connection to an Azure ExpressRoute
   - Private Peering Connection to an Azure ExpressRoute

Configure Prerequisites for Cisco SD-WAN Cloud Interconnect with Equinix

Associate Equinix Account with Cisco SD-WAN Manager

Prerequisites

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.
2. After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* information in the Equinix Developer Platform Knowledge Center.
3. Create billing accounts for each region in which you would like to deploy an Interconnect Gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Associate Interconnect Account**.
4. Configure the following:

Interconnect Provider	Choose **EQUINIX**.
Account Name	Enter a name of your choice. This name is used to identify the Equinix account in workflows that define the cloud or site-to-site interconnects.
Description (Optional)	Enter a description.
Customer Key	Enter the client ID (consumer key).
Customer Secret	Enter the client secret key (consumer secret).

5. Click **Add**.

Cisco SD-WAN Manager authenticates the account and saves the account details in a database.

Configure Global Settings for Equinix Interconnect Gateways

Prerequisites

1. Create an account on the Equinix portal. Refer to the *New User Equinix Fabric Portal Access* documentation from Equinix.

2. After creating the account, generate the client ID (consumer key) and client secret key (consumer secret) for the account. Refer to the *Generating Client ID and Client Secret Key* information in the Equinix Developer Platform Knowledge Center.
3. Create billing accounts for each region in which you would like to deploy an Interconnect Gateway using this account. Refer to the *Billing Account Management* documentation from Equinix.
4. Associate Equinix account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Global Settings**.
   - To add global settings, click **Add**.
   - To modify global settings, click **Edit**.
4. Configure the following:

Enable Configuration Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, enable this option to use configuration groups to configure devices in the multicloud workflow. This option is disabled by default. **Note** When you enable configuration groups here, configuration groups are enabled for all cloud providers. For example, enabling this option here also enables it for all other multicloud and interconnect providers.
Interconnect Provider	Choose **EQUINIX**.
Software Image	Choose a Cisco CSR 1000v image. For Cisco Catalyst SD-WAN Manager Release 20.12.1, choose a Cisco Catalyst 8000v image.
Instance Size	Instance size determines the compute footprint and throughput of each Cisco CSR 1000v instance.
Interconnect Transit Color	Choose the color to be assigned for connection between Interconnect Gateways. This color is restricted to prevent direct peering between branch locations. Do not assign the same color to another connection in the Cisco Catalyst SD-WAN fabric. **Note** It is recommended to use private colors. Do not use default colors.
BGP ASN	Enter a BGP ASN for peering between Interconnect Gateway and cloud provider. You can enter an ASN of your choice or reuse an existing ASN used by your organization.

Interconnect CGW SDWAN Color	Minimum supported release: Cisco vManage Release 20.9.1 Choose the color to be used for the interface through which the interconnect gateway connects to the cloud gateway. **Note** Color assigned to an interface must be unique for the interconnect gateway devices and common across cloud interconnect providers. For Microsoft Azure deployments, Cisco Catalyst SD-WAN tunnel color is not configured on the WAN interface of the cloud gateway through automation and you must manually update the WAN interface color. Ensure that the template color matches the color of the branch router, interconnect gateway, and cloud gateway.

5. To save the newly added global settings, click **Save**.

   To save the modified global settings, click **Update**.

Attach Equinix Template to Cisco CSR 1000v or Cisco Catalyst 8000v Instance

Note This procedure is not required if you enabled configuration groups. In this case, skip to Create Interconnect Gateway at an Equinix Location.

Before you can deploy a Cisco CSR 1000v instance as an interconnect gateway at an Equinix location, you must attach the Equinix default template to the device. We recommend that you attach the template named *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02.*

For Cisco Catalyst SD-WAN Manager Release 20.12.1, the default template for Cisco Catalyst 8000v is *Default_EQUINIX_ICGW_C8000V_Template_V01*.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

3. Choose the **Template Type** as **Default** and find the template named *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02.*

   For Cisco Catalyst SD-WAN Manager Release 20.12.1, choose the default *Default_EQUINIX_ICGW_C8000V_Template_V01*.
4. Click **…** and click **Attach Devices**.
5. Choose the UUID of desired Cisco CSR 1000v instance from the list of **Available Devices** and move the instance to the list of **Selected Devices**.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.

6. Click **Attach**.
7. The template contains variables. To enter values for the variables in the template, click **…** and click **Edit Device Template**.
8. Enter the values for the following variables and click **Update**:
   - DNS Address (vpn_dns_primary)
   - DNS Address (vpn_dns_secondary)
   - Color (vpn_if_tunnel_color_value)
   - System IP (system-ip)
   - Site ID (site-id)
   - Hostname (host-name)
9. Click **Next**.
10. Click **Configure Devices**.

Create Interconnect Gateway at an Equinix Location

Deploy a Cisco CSR 1000v instance as the interconnect gateway at the desired Equinix location. We recommend that you deploy the Cisco CSR 1000v instance at an Equinix location closest to your branch location.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can deploy a Cisco Catalyst 8000v instance.

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. If you did not enable configuration groups, attach the Equinix template to the Cisco CSR 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach the template to the Cisco Catalyst 8000v instance.
4. If you enabled configuration groups, ensure that you configure device parameters for devices that are associated with the configuration group.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Create Interconnect Gateway**.
4. Configure the following:

Interconnect Provider	Choose **EQUINIX**.

Gateway Name	Enter a name to uniquely identify the gateway.
Description (Optional)	Enter a description.
Account Name	Choose an Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose the Equinix location where the Cisco CSR 1000v instance must be deployed. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.
Billing Account ID	Choose the appropriate billing account for the location.
Site Name	Choose the site. Starting Cisco vManage Release 20.10.1, Site Name field is available.
Configuration Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you enabled the **Enable Configuration Group** option when you created a cloud gateway or configured global settings for interconnect gateways, perform one of these actions: • Choose a configuration group. • To create and use a new configuration group, choose **Create New**. In the **Create Configuration Group** dialog box, enter a name for a new configuration group and click **Done**. Choose the new configuration group from the drop-down list. The configuration group that you choose is used to configure devices in the multicloud workflow. For more information about configuration groups, see Cisco Catalyst SD-WAN Configuration Groups. **Note** • The **Configuration Group** drop-down list includes only configuration groups that you create from this drop-down list. It does not include other configuration groups that have been created in Cisco Catalyst SD-WAN. The configuration groups in this drop-down list include the options that are needed for this provider. • If you create the Equinix Interconnect Gateway by using a configuration group, using SSH from Cisco SD-WAN Manager works only when the interconnect gateway is Cisco Catalyst 8000v 17.13 or later.

UUID	Choose the UUID of a Cisco CSR 1000v instance that has the Equinix default template attached. **Note** When a site name is selected, UUID field is auto-populated with the UUID associated with the site name. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.
Settings	Choose one of the following: • **Default**: Use instance size and software image defined in the Interconnect Global Settings. • **Custom**: Choose a specific instance size and software image for this gateway.

5. Click **Add**.

When the configuration task is successful, the interconnect gateway is listed in the **Gateway Management** page.

Note Before proceeding further, verify that the **Device Status** column for the interconnect gateway shows **In Sync** and the certificate is successfully installed.

Create Interconnect to AWS

Associate AWS Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud**.
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Amazon Web Services**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Log in to AWS with	Choose **Key** or **IAM Role**.
Role ARN	Enter the API/Secret Key or the Role ARN.

5. Click **Add**.

Cisco SD-WAN Manager uses the API/Secret Key or the Role ARN to authenticate the user account with AWS as part of the API workflow to create connections to AWS.

Discover Host Private Networks and Tag AWS VPCs

A number of host VPCs can be grouped together using a tag. VPCs under the same tag are considered as a singular unit. Tag the AWS VPCs to which you wish to create software-defined cloud interconnects from an interconnect gateway.

Prerequisite

Associate AWS Account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Amazon Web Services**.

   The available host VPCs are discovered and listed in a table.

   The host VPC table includes the following columns:

   - Cloud Region
   - Account Name
   - Host VPC Name
   - Host VPC Tag
   - Interconnect Enabled
   - Account ID
   - Host VPC ID

5. Select the VPCs that you wish to tag using the check boxes in the left-most column.
6. Click **Tag Actions**.

   You can perform the following actions:

   - Add Tag - group the selected VPCs and tag them together.
   - Edit Tag - migrate the selected VPCs from one tag to another.
   - Delete Tag - remove the tag for the selected VPCs.

7. Click **Add Tag** and configure the following:

Tag Name	Enter a name for the tag that links the selected VPCs.
Region	List of regions that correspond to the selected VPCs. Click **X** to omit a region and associated VPCs from the tag.

Selected VPCs	List of VPC IDs of the selected host VPCs. Click **X** to omit a VPC from the tag.
(Cisco vManage Release 20.8.1 and earlier) Enable for Interconnect Connectivity (From Cisco vManage Release 20.9.1) Enable for SDCI partner Interconnect Connections	To use the VPC tag while creating a cloud interconnect connection to AWS, check the check box. If enabled, the tag can only be used for cloud interconnect connections and is not available for Multicloud Gateway Intent Mapping. If you do not check the check box, you cannot use the VPC tag to create a cloud interconnect connection. **Note** Do not enable this setting when you use cloud gateways to connect VPC workloads. You cannot edit this setting when the tag is in use by a connection.

8. Click **Add**.

On the **Discover Host Private Networks** page, the VPCs you selected earlier are tagged and the tag name is shown in the **Host VPC Tag** column. If you chose to use the VPC tag for software-defined cloud interconnects, the **Interconnect Enabled** column reads **Yes**.

Create Direct Connect Public Hosted Connection to AWS from Interconnect Gateway

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Attach Equinix Template to Cisco CSR 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
6. Create interconnect gateway at an Equinix Location.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.

6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the direct connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

9. Configure the following and click **Next**:

Equinix Hosted Connection VIF Type	Choose **Public**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.
Interconnect IP Address	Enter the public IP Address (CIDR) to be used as the BGP Peer ID of the interconnect gateway.
Amazon IP Address	Enter the public IP Address (CIDR) to be used as the AWS BGP Peer ID.
Prefixes	Enter the summary AWS addresses and prefixes you wish to advertise to the branch location.
Segment	Choose the segment ID for this connection.

10. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Private Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect Gateways.

3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag AWS VPCs.
6. Attach Equinix template to Cisco CSR1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
7. Create Interconnect Gateway at an Equinix Location.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the Interconnect Gateway from which the Direct Connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

9. Configure the following and click **Next**:

Equinix Hosted Connection VIF Type	Choose **Private**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.

Direct Connect Gateway	**a.** Click the Refresh button to fetch the Direct Connect gateways associated with the selected AWS account. **b.** Choose the direct connect gateway to which the direct connect connection must be created. Alternatively, create a new direct connect gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.

Settings	Choose one of the following:
	• **Global**:
	  • BGP peering IP address is picked from an internally reserved /16 subnet (198.18.0.0/16).
	  • BGP ASN is picked from the Global Settings.
	• **Custom**:
	  • Enter a custom /30 CIDR IP address for BGP peering.
	  • Enter custom BGP ASN for peering.
	
	Note
	You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.

Attachment	Cisco vManage Release 20.8.1 and earlier: Choose **VPC**. **Segment**: Choose the segment ID for this connection. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection.
	Cisco vManage Release 20.9.1 and later: Choose one of the following: • **VPC** **Segment**: Choose the segment ID for this connection. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. • **Cloud Gateway** **Cloud Gateways**: Choose the cloud gateways to attach to this connection. If the drop-down is empty, you must first create the cloud gateway using the multicloud workflows. For a single connection, AWS supports up to 10 cloud gateways. Each cloud gateway can be connected to 30 interconnect connections.

10. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Direct Connect Transit Hosted Connection to AWS Direct Connect Gateway from Interconnect Gateway

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate AWS Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and Tag AWS VPCs.
6. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.

   Attach Equinix Template to Cisco CSR 1000v Instance for versions prior to Cisco Catalyst SD-WAN Manager Release 20.12.1.

7. Create Interconnect Gateway at an Equinix Location.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the direct connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **AWS**.
Connection Name	Enter a unique name for the connection.
AWS Account	Choose an AWS account by the account name entered while associating the AWS account details on Cisco SD-WAN Manager.

9. Configure the following and click **Next**:

Equinix Hosted Connection VIF Type	Choose **Transit**.
Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose an AWS Direct Connect location.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.
Direct Connect Gateway	**a.** Click the Refresh button to fetch the direct connect gateways associated with the selected AWS account. **b.** Choose the Direct Connect Gateway to which the direct connect connection must be created. Alternatively, create a new Direct Connect Gateway by clicking **Add New Direct Connect Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Click **Save**.

Settings	Choose one of the following:
	• **Global**:
	  • BGP peering IP address is picked from an internally reserved /16 subnet (198.18.0.0/16).
	  • BGP ASN is picked from the Global Settings.
	• **Custom**:
	  a. Enter a custom /30 CIDR IP address for BGP peering.
	  b. Enter custom BGP ASN for peering.
	  Note You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently.

Segment	Choose the segment ID for this connection.
Attachment	Choose **Transit Gateway**. **Transit Gateway**: **a.** Click the Refresh button to fetch the transit gateways associated with the selected AWS account. **b.** Choose the transit gateway to which the direct connect connection must be created. Alternatively, create a new transit gateway by clicking **Add New Transit Gateway**. **a.** Enter a **Gateway Name**. **b.** Enter a **BGP ASN** for the gateway. **c.** Select **AWS Region**. **d.** Click **Save**. **VPC Tags**: Choose VPC tags to identify VPCs for which traffic must be routed through this connection. **Allowed Prefixes**: **a.** Click **Add Prefixes**. **b.** Enter the IPv4 CIDR prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard.

10. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Create Interconnects to Google Cloud

Associate Google Cloud Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud** .
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Google Cloud**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.
Private Key ID	Click **Upload Credential File**. You must generate this file by logging in to the Google Cloud console. The private key ID may be in the JSON or the REST API format. The format depends on the method of key generation. For more details, see Google Cloud documentation.

5. Click **Add**.

Cisco SD-WAN Manager uses the Private Key ID to authenticate the user account with Google Cloud as part of the workflow to create connections to Google Cloud.

Create Interconnect to Google Cloud Routers from Interconnect Gateways

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Deploy Google Cloud Routers in network-regions to which you wish to connect.

   For nonredundant connectivity, on the Google Cloud console, deploy a Google Cloud Router in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

For redundant connectivity, on the Google Cloud console, deploy two Google Cloud Routers in each network-region to which you wish to connect and create a VLAN attachment for each Google Cloud Router.

Starting from Cisco vManage Release 20.9.1, you can create the Google Cloud Routers and VLAN attachments fromCisco SD-WAN Manager during connection creation.



Note For use with interconnect attachments, you must set the Google ASN for the Google Cloud Routers to 16550.

3. Associate Equinix Account with Cisco SD-WAN Manager.
4. Configure Global Settings for Interconnect Gateways.
5. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
6. Create Interconnect Gateway at a Equinix Location closest to your Cisco Catalyst SD-WAN branch location.

   For redundant connectivity to Google Cloud, create a pair of interconnect gateways in the Equinix fabric. For nonredundant connectivity, deploy an interconnect gateway at a Equinix location.
7. Create necessary network segments (see Segmentation Configuration Guide).
8. Associate Google Cloud Account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Google Cloud**.
Google Account	Choose a Google account by the account name entered while associating the Google account details with Cisco SD-WAN Manager.

Attachment	Minimum supported release: Cisco vManage Release 20.9.1 Choose **Shared VPC** to attach a Google Cloud Router and Google Cloud Interconnect to the connection..
Region	Minimum supported release: Cisco vManage Release 20.9.1 Choose a Google Cloud region.
VPC Network	Minimum supported release: Cisco vManage Release 20.9.1 Choose the VPC network to deploy this connection.

Redundancy	For Cisco vManage Release 20.8.1 and earlier: Choose **Enable** if you want to create connections with redundancy. **Primary Google Cloud Interconnect Attachment:** • Click the refresh symbol next to the **Primary Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*. **Secondary Google Cloud Interconnect Attachment:** • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*. The secondary interconnect attachment options are determined based on the region and network to which the primary interconnect attachment belongs. If you do not have an unused interconnect attachment in the same region and network as the primary interconnect attachment, the drop-down list is empty and indicates that you must create a redundant interconnect attachment on the Google Cloud portal. Choose **Disable** if you want to create the connection without redundancy. **Google Cloud Interconnect Attachment**: • Click the refresh symbol next to the **Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment. The interconnect attachment name has the format *<region-name>::<cloud-router-name>::<interconnect-attachment-name>*.

	For Cisco vManage Release 20.9.1 and later: **Google Cloud Router**: • Click the refresh symbol next to the **Google Cloud Router** drop-down list. • Choose a Google Cloud router or click **Add New Google Cloud Router**. If you clicked **Add New Google Cloud Router**, configure the router settings in the **Add Google Cloud Router** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud router region. • VPC Network: Choose the Google Cloud router network. • Cloud Router Name: Enter a unique Google Cloud router name. **Note** Google Cloud routers are always created with a BGP ASN of 16550, MTU of 1500 and with default routing enabled. **Google Cloud Interconnect Attachment**: • Click the refresh symbol next to the **Google Cloud Interconnect Attachment** drop-down list. • Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the router settings in the **Add Google Cloud Interconnect Attachment** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud Interconnect attachment region. • VPC Network: Choose the Google Cloud network for the interconnect attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network for the interconnect attachment. • IC Attachment Name: Enter a unique name for the interconnect attachment. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.

9. Configure the following settings for the primary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the primary VLAN attachment.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

10. If you enabled redundancy in Step 8, configure the following settings for the secondary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the secondary VLAN attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary VLAN attachment.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which a connection must be established to the secondary VLAN attachment.

11. Configure the following and click **Next**:

Settings	Choose **Auto-generated** or **Custom**. • **Auto-generated:** The Interconnect BGP ASN is selected by the system • **Custom**: Specify Interconnect BGP ASN of your choice for peering with the interconnect VLAN attachments. **Note** You can specify a custom BGP ASN only for the first interconnect from an Interconnect Gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. BGP peering IP addresses for interconnects to Google Cloud Routers are auto-assigned by Google from the subnet (169.254.0.0/16). The IP addresses cannot be configured from Cisco SD-WAN Manager.
Segment	Choose a segment ID for this connection.

12. Review the connection summary.

- To create the connection, click **Save**.

- To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched and creates the interconnects between the Interconnect Gateway and the interconnect attachments of the Google Cloud routers.

When the task is successful, the connections are listed on the **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

What to do Next: On the Google Cloud console, manage the routes advertised from the Google Cloud Routers towards the interconnect gateway via BGP.

Create Interconnect Connection to a Cloud Gateway In Google Cloud

Prerequisites

1. Create the required VPC network using the Google Cloud console.
2. Associate Equinix Account with Cisco SD-WAN Manager.
3. Configure Global Settings for interconnect gateways.
4. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, choose Cisco Catalyst 8000v instance.
5. Create Interconnect Gateway at a Equinix Location closest to your Cisco Catalyst SD-WAN branch location.

   For redundant connectivity to Google Cloud, create a pair of interconnect gateways in the Equinix fabric. For nonredundant connectivity, deploy an interconnect gateway at a Equinix location.
6. Create necessary network segments (see Segmentation Configuration Guide).
7. Associate Google Cloud Account with Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.

Cloud Service Provider	Choose **Google Cloud**.
Google Account	Choose a Google account by the account name entered while associating the Google account details with Cisco SD-WAN Manager.
Attachment	Choose **Cloud Gateway** to connect to a Cloud Gateway. **Cloud Gateways**: You can select only one Cloud Gateway from the drop-down list.

9. Configure the following and click **Next**:

PRIMARY	
Google Cloud Router	Choose the Google Cloud router.
Google Cloud Interconnect Attachment	Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the router settings in the **Add Google Cloud Interconnect Attachment** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud Interconnect attachment region. • VPC Network: Choose the associated network to the attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network. • ID Attachment Name: Enter a unique attachment name. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.
SECONDARY	
Google Cloud Router	Choose the Google Cloud router.

Google Cloud Interconnect Attachment	Choose the desired interconnect attachment or click **Add New Google Cloud Interconnect Attachment**. If you clicked **Add New Google Cloud Interconnect Attachment**, configure the router settings in the **Add Google Cloud Interconnect Attachment** slide-in pane. Configure the following and click Save: • Region: Choose the Google Cloud Interconnect attachment region. • VPC Network: Choose the associated network to the attachment. • Cloud Router Name: Choose the Google Cloud router deployed for the selected region and VPC network. • ID Attachment Name: Enter a unique attachment name. • Secondary Zone: If you want to deploy this attachment on the secondary zone, check the checkbox.

10. Configure the following settings for the primary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the primary VLAN attachment.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen peering location.

11. If you enabled redundancy in Step 8, configure the following settings for the secondary VLAN attachment and click **Next**:

Peering Location	**a.** Click the Refresh button to update the list of available locations. **b.** Choose a Equinix location closest to the GCP region where you created the Google Cloud Router and the secondary VLAN attachment. **Tip** For redundancy, choose a location other than the peering location associated with the primary VLAN attachment.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which a connection must be established to the secondary VLAN attachment.

12. Configure the following and click **Next**:

Settings	Choose **Auto-generated** or **Custom**. • **Auto-generated:** The Interconnect BGP ASN is selected by the system • **Custom**: Specify Interconnect BGP ASN of your choice for peering with the interconnect VLAN attachments. **Note** You can specify a custom BGP ASN only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. BGP peering IP addresses for interconnects to Google Cloud Routers are auto-assigned by Google from the subnet (169.254.0.0/16). The IP addresses cannot be configured from Cisco SD-WAN Manager.
Segment	Choose a segment ID for this connection.

13. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

    When you save the connection configuration, a configuration task is launched and creates the interconnects between the interconnect gateway and the interconnect attachments of the Google Cloud routers.

    When the task is successful, the connections are listed on the **Interconnect Connectivity** page. You can also view the connection details on the Google Cloud console.

What to do Next: On the Google Cloud console, manage the routes advertised from the Google Cloud Routers towards the interconnect gateway via BGP.

Create Interconnects to Microsoft Azure

Associate Microsoft Azure Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Cloud** .
3. Click **Associate Cloud Account**.
4. Configure the following:

Cloud Provider	Choose **Microsoft Azure**.
Cloud Account Name	Enter a name of your choice.
Description (Optional)	Enter a description.
Use for Cloud Gateway	Choose **No**.

Tenant ID	Enter the ID of your Azure Active Directory (AD). **Tip** To find the tenant ID, go to your Azure Active Directory and click **Properties**.
Subscription ID	Enter the ID of the Azure subscription you want to use.
Client ID	Enter your existing Azure application ID. See Azure documentation for more information on how to register an application in Azure AD, get the client ID and secret key, and more.
Secret Key	Enter the password associated with the client ID.

5. Click **Add**.

Discover Host Private Networks and Tag Microsoft Azure VNets

Tag the Microsoft Azure VNets to which you wish to create software-defined cloud interconnects from an interconnect gateway. Azure VNets grouped using the same VNet tag are considered a singular unit.

Prerequisite

Associate Microsoft Azure Account with Cisco SD-WAN Manager.

Add a Tag

Group VNets and tag them together.

Note VNets belonging to different resource groups cannot be used together.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Choose the Azure VNets that you wish to tag by checking the corresponding check boxes.
6. Click **Tag Actions**.
7. Click **Add Tag** and configure the following:

Field	Description
Tag Name	Enter a name for the tag.

Field	Description
Region	If you selected VNets before clicking **Add Tag**, this field shows the list of regions that correspond to the selected VNets. • If you did not select VNets before clicking **Add Tag** or wish to select more regions, choose regions from the drop-down list. • Click **X** to omit a region and associated VNets from the tag.
Selected VNets	If you selected VNets before clicking **Add Tag**, this field shows the list of VNet IDs of the selected host VNets. • If you did not select VNets before clicking **Add Tag** or wish to select more VNets, choose VNets from the drop-down list. • Click **X** to omit a VNet from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	To use the VNets tag while creating interconnect connections to Microsoft Azure, check the check box. If enabled for interconnect connetions, the tag cannot be used in the Microsoft Azure Multicloud workflow. If not enabled for interconnect connections, the tag can only be used with Microsoft Azure Multicloud workflow. **Note** Do not enable this setting when you use Cloud Gateways to connect VNet workloads.

8. Click **Add**.

On the **Host Private Networks** page, the Azure vNets you selected earlier are tagged and the tag name is shown in the **VNET Tag** column. If you chose to use the vNet tag for cloud interconnects, the **Interconnect Enabled** column reads **Yes**.

Edit a Tag

Add VNets to or remove VNets from an existing tag.

From Cisco vManage Release 20.10.1, edit a VNet tag associated with an interconnect connection subject to the following conditions:

- If only one VNet is associated with a VNet tag, you cannot remove the VNet from the tag. To remove the VNet from the tag, delete the interconnect connection and then edit the tag.
- For a private-peering connection with a virtual WAN attachment, the VNets you wish to associate with the tag must be from the same regions as the VNets already associated with the tag.

  To attach VNets from a new region to the private-peering connection, do the following:

  1. Create a new tag for the region and associate required VNets.
  2. Edit the private-peering connection and attach the VNet tag to the connection.

- For a private-peering connection with a VNet attachment, you can associate VNets from a new region to the tag while editing the tag.



Note In Cisco vManage Release 20.9.1 and earlier releases, you cannot edit a VNet tag that is associated with an interconnect connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Edit Tag** and modify the following as required:

Field	Description
Tag Name	From the drop-down list, choose a tag name.
Region	This field shows the list of regions that correspond to the VNets associated with the tag. • Choose additional regions from the drop-down list. • Click **X** to omit a region and associated VNets from the tag.
Selected VNets	This field shows the list of VNets associated with the tag. • Choose additional VNets from the drop-down list. • Click **X** to omit a VNet from the tag.
(From Cisco vManage Release 20.9.1) **Enable for SDCI partner Interconnect** Connections (Cisco vManage Release 20.8.1 and earlier) **Enable for Interconnect Connectivity**	(Read only) Indicates whether the VNet is configured to be used while configuring interconnect connections or for Multicloud Gateway intent mapping.

7. Click **Update**.

Delete a Tag

Remove a tag that groups together VNets.

Note You cannot delete a VNet tag while the tag is associated with an interconnect connection.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Host Private Networks**.
4. **Cloud Provider**: choose **Microsoft Azure**.

   The available host VNets are discovered and listed in a table.
5. Click **Tag Actions**.
6. Click **Delete Tag**.
7. **Tag Name**: From the drop-down list, choose a tag name.
8. Click **Delete**.

Create Microsoft-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
6. Create Interconnect Gateways at Equinix Location.

   For connectivity to Microsoft Azure, create a pair of interconnect gateways in the Equinix fabric. Redundant connectivity is the default and only supported configuration.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: Choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.

6. **Choose Interconnect Gateway**: Choose the Interconnect Gateway from which the connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Microsoft Azure**.
Azure Account	Choose a Microsoft Azure account by the account name entered while associating the account details with Cisco SD-WAN Manager.

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following and click **Save**: • Resource Group: Choose a resource group associated with the Microsoft Azure account. • Region: Choose an Azure region. • Instance Name: Enter a name for the ExpressRoute instance. • Provider: Choose **Equinix**. • Peering Location: Click the Refresh button to update the list of available locations. Choose an ExpressRoute location. • Bandwidth: Choose the bandwidth of the ExpressRoute circuit. • SKU: Choose the **Premium** or the **Standard** SKU. • Billing Model: Choose **Metered** billing or **Unlimited**.

9. Configure the following settings for the primary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

10. Configure the following settings for the secondary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	The bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which the secondary connection must be established.

11. Configure the following and click **Next**:

Deployment Type	Choose **Public**.
Primary IPv4 Subnet	Enter a /30 CIDR public IP address for BGP peering from the primary interconnect gateway. Before creating the connection, ensure that your organization is permitted to use the public IPv4 address.
Secondary IPv4 Subnet	Enter a /30 CIDR public IP address for BGP peering from the secondary interconnect gateway. Before creating the connection, ensure that your organization is permitted to use the public IPv4 address.
BGP Advertise Prefix	Enter the summary addresses and prefixes you wish to advertise to the interconnect gateway.
Segment	Choose a segment ID for this connection.

12. Review the connection summary.
    - To create the connection, click **Save**.
    - To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched. This task creates the following resources:

- virtual cross connects in the Equinix fabric between the interconnect gateways and the ExpressRoute
- Microsoft Azure public/private peerings for ExpressRoute circuits
- a vNet gateway, if a vNet gateway does not exist for a vNet
- connections between the ExpressRoute and the vNet gateways

When the task is successful, the connections are listed on the **Interconnect Connectivity** page.

You can also view the connection details on the Microsoft Azure portal.

Create Private-Peering Connection to Microsoft Azure ExpressRoute from Interconnect Gateways

Prerequisites

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Associate Microsoft Azure Account with Cisco SD-WAN Manager.
5. Discover Host Private Networks and tag Microsoft Azure VNets.
6. Attach Equinix Template to Cisco Catalyst 1000v Instance.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, attach Cisco Catalyst 8000v instance.
7. Create Interconnect Gateways at Equinix Location.

   For connectivity to Microsoft Azure, create a pair of interconnect gateways in the Equinix fabric. Redundant connectivity is the default and only supported configuration.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **Equinix**.
5. **Choose Interconnect Account**: choose a Equinix account by the account name entered while associating the account details on Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the interconnect gateway from which the direct connect connection must be created.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Cloud**.
Cloud Service Provider	Choose **Microsoft Azure**.
Azure Account	Choose a Microsoft Azure account by the account name entered while associating the account details with Cisco SD-WAN Manager.

ExpressRoute	**a.** Click the Refresh button to update the list of available ExpressRoutes **b.** Choose an ExpressRoute or click **Add New ExpressRoute**. **Note** • Starting from Cisco vManage Release 20.8.1, Equinix ExpressRoutes are available. • Starting from Cisco vManage Release 20.8.1, all the ExpressRoutes created for the respective interconnect providers displayed in the list of available ExpressRoutes drop-down are color-coded depending on their provisioning status. Here is the list of colors and their significance, • Black: Not Provisioned. • Grey: Provisioned. • Red: Failed. • Only the non-provisioned ExpressRoutes from the chosen Azure account are available for selection. You can check the state of ExpressRoutes on the Microsoft Azure portal. If you clicked **Add New ExpressRoute**, configure the ExpressRoute settings in the **Create New ExpressRoute** slide-in pane. Configure the following and click **Save**: • Resource Group: Choose a resource group associated with the Microsoft Azure account. • Region: Choose an Azure region. • Instance Name: Enter a name for the ExpressRoute instance. • Provider: Choose **Equinix**. • Peering Location: Click the Refresh button to update the list of available locations. Choose an ExpressRoute location. • Bandwidth: Choose the bandwidth of the ExpressRoute circuit. • SKU: Choose the **Premium** or the **Standard** SKU. • Billing Model: Choose **Metered** billing or **Unlimited**.

9. Configure the following settings for the primary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	Choose the connection bandwidth (in Mbps). The list of permitted bandwidth values is populated based on the chosen ExpressRoute.

10. Configure the following settings for the secondary connection to the ExpressRoute and click **Next**:

Peer Location	The location is chosen automatically based on the ExpressRoute you chose earlier.
Connection Name	Enter a unique name for the connection.
Bandwidth (Mbps)	The bandwidth of the secondary connection is set to the same value as that of the primary connection.
Source Gateway	Choose the interconnect gateway from which the secondary connection must be established.

11. Configure the following and click **Next**:

Deployment Type	Choose **Private**.
BGP-Peering Settings	Choose **Auto-generated** or **Custom**. **Auto-generated**: The interconnect BGP ASN, and the primary and secondary IPv4 subnets are selected by the system. The IPv4 subnets are selected from an internally reserved /16 subnet (198.18.0.0/16). **Custom**: **Note** You can specify a custom BGP ASN and custom IPv4 subnets only for the first interconnect from an interconnect gateway. After an interconnect is created from an interconnect gateway, the BGP ASN cannot be modified for any interconnects created subsequently. • **BGP ASN**: Specify an ASN of your choice for the primary and secondary peering with the ExpressRoute. • **Primary IPv4 Subnet**: Enter a /30 CIDR IP address for BGP peering with the primary interconnect gateway. • **Secondary IPv4 Subnet**: Enter a /30 CIDR IP address for BGP peering with the secondary interconnect gateway.
Attachment	Choose one of the following: • **vNet**: Attach VNets to the connection using VNet tags. • **vWAN**: Attach virtual WAN to the connection and choose VNets from the regions of the virtual WAN using VNet tags. • Minimum supported release: Cisco vManage Release 20.9.1 **Cloud Gateway**: Attach cloud gateways to the connection. You can select upto 5 cloud gateways per connection.
VNet Settings	**VNet Tags**: Choose VNet tags to identify VNets for which traffic must be routed through this connection.

virtual WAN Settings	**vWAN**: Choose or add a new virtual WAN. **Note** You can choose the virtual WAN to be attached only for the first connection to Microsoft Azure from an interconnect gateway for the selected resource group of the ExpressRoute Circuit. The same virtual WAN is attached to any subsequent connection in the same resource group to which you choose to attach a virtual WAN. Starting from Cisco vManage Release 20.8.1, Cisco SD-WAN Manager supports one virtual WAN per Microsoft Azure resource group per Microsoft Azure account. Once that vWAN is chosen and used as part of a virtual WAN connection, subsequent virtual WAN connections to the same Microsoft Azure resource group use the same virtual Wan. The Microsoft Azure resource group is determined for the connection when the ExpressRoute Circuit is selected for it. All other Microsoft Azure resources belonging to the connection must be in the same Microsoft Azure resource group as that of the selected ExpressRoute Circuit. **vNet**: Choose VNet tags to identify VNets for which traffic must be routed through this connection. Cisco SD-WAN Manager finds VNets based on the chosen VNet Tags, and identifies the regions to which the VNets belong. For the chosen virtual WAN and the identified regions, Cisco SD-WAN Manager finds and lists the available virtual hubs for verification. For regions where a virtual hub does not exist, you must specify the name and address-prefix to add a virtual hub. **vHub Settings**: **Note** From Cisco Catalyst SD-WAN Manager Release 20.12.1, if multiple Azure Virtual WAN hubs are there in a region, you can select a particular Azure Virtual WAN hub for that region. Once you choose the Azure Virtual WAN hub, all subsequent connections created for Azure Virtual WAN uses the same Azure Virtual WAN hub. **a.** Click **Add Settings**. Or, if you're modifying the configuration, click **Edit Settings**. **b.** Review the virtual hub name and address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.
Segment	Choose a segment ID for this connection.

12. Review the connection summary.

- To create the connection, click **Save**.
- To modify the connection settings, click **Back**.

When you save the connection configuration, a configuration task is launched.

For VNet attachmment, the configuration task creates the following resources:

- virtual cross connects in the Equinix fabric between the interconnect gateways and the ExpressRoute
- Microsoft Azure public/private peerings for the ExpressRoute circuits
- a vNet gateway, if a vNet gateway does not exist for a vNet
- connections between the ExpressRoute and the vNet gateways

For virtual WAN attachment, the configuration task creates the following resources:

- virtual cross connects in the Equinix fabric between the interconnect gateways and the ExpressRoute
- Microsoft Azure public/private peerings for the ExpressRoute circuits
- necessary virtual hubs
- connections between vNets and virtual hubs
- an ExpressRoute Gateway for each virtual hub, if necessary
- connections between the ExpressRoute Gateway and ExpressRouteCircuits

When the task is successful, the connections are listed on the **Interconnect Connectivity** page.

You can also view the connection details on the Microsoft Azure portal.

Device Links

Device link groups create a full-mesh network between two or more edge devices. Device links connects all the edge devices, that are part of a group, together to create a WAN. All the device links in a mesh share the same bandwidth between the edge devices.

Note

- Only one device link is supported per Equinix account.
- Point to point connection cannot be formed between interconnect gateways belonging to a device link group.
- When you upgrade to Cisco vManage Release 20.9.2 and Cisco vManage Release 20.10.1, you have to modify the device link by adding or removing some devices to push new configuration to the devices. Otherwise, the BFD session for site-to-site connection goes down when site-to-site and device link are present on the same Interconnect Gateway.

Add Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. Click **Device Links**.
5. Click **Add Device Links**.
6. Choose **Account name** from the drop down menu. This is the Equinix account that has been associated to Cisco SD-WAN Manager through Account Association.
7. Enter **Device link name**.
8. Choose **Bandwidth** from the drop down menu.

Note The maximum bandwidth supported by Equinix is 10000 Mbps per metro.

9. (Optional)

   Enter **Subnet**.

Note
- Provide IP subnets for interconnect gateway device link interface.
- The subnet should be in 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 range.
- The subnet should not conflict with 172.31.251.0/21.
- The subnet should not conflict with other connections.
- If you do not enter the subnet, 198.19.0.0/16 is used by default.

10. Select **Gateway Name** from the drop down menu. Select at least two gateway names.
11. Click **Save**.

Delete Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. Click **Device Links**.

   Existing device links are summarized in a table.
5. In the table, find the desired link and click **...**.

6. To delete a device link, click **Delete** and confirm that you wish to delete the device link.

Update Device Links

1. From the Cisco SD-WAN Manager menu, go to **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. Click **Device Links**.

   Existing device links are summarized in a table.
5. In the table, find the desired link and click **...**.
6. To edit the device link, click **Edit**.
7. In the **Edit Device Link** page, you can only update the **Bandwidth** and **Gateway Name** to add or remove gateways.



Note Bandwidth and Gateway Name are the only two parameter that can be edited.

When adding or removing devices, at least two devices should be present in the device link.

The maximum bandwidth supported by Equinix is 10000 Mbps per metro.

8. Click **Save**.

Create Interconnect Between Interconnect Gateways

From Cisco SD-WAN Manager, you can create an interconnect between interconnect gateways at two or more Equinix locations. By doing so, you can link the SD-WAN branch locations connected to these interconnect gateways via the Equinix fabric.

Prerequisites

For each SD-WAN branch location to be connected through the Equinix fabric, complete the following configuration prerequisites:

1. Associate Equinix Account with Cisco SD-WAN Manager.
2. Configure Global Settings for interconnect gateways.
3. Create necessary network segments (see Segmentation Configuration Guide).
4. Identify the nearest Equinix location.
5. Create an Interconnect Gateway at the Equinix location closest to the branch location.

Note If you have a VRF defined in two branch locations and wish to exchange traffic attached to the VRF through the connection between the interconnect gateways, you must configure the VRF and an appropriate centralized policy on the interconnect gateways to route the branch traffic through the connection between the interconnect gateways.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.
4. **Choose Interconnect Provider**: choose **EQUINIX**.
5. **Choose Interconnect Account**: choose an Equinix account by its account name; the account name is the name you entered while associating the account with Cisco SD-WAN Manager.
6. **Choose Interconnect Gateway**: choose the source interconnect gateway.
7. Click **Add Connection**.
8. Configure the following and click **Next**:

Destination Type	Choose **Edge**.
Connection Name	Enter a unique name for the connection.
Interconnect Gateway	Choose destination interconnect gateway.
Bandwidth	Choose the connection bandwidth. Unit: Mbps.

Note Interconnect gateways belonging to a device link group cannot be used to form a point to point connection.

9. Review the connection summary.
   - To create the connection, click **Save**.
   - To modify the connection settings, click **Back**.

When the configuration task is successful, the connection is listed in the **Interconnect Connectivity** page.

Verify and Modify Configuration for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

View Interconnect Gateway and Connection Summary

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud** > **Interconnect**. On this page, you can view a summary of the interconnect gateways and connections that you have created. If you have not created any interconnect gateways, page provides an overview of the workflow for creating and managing interconnect gateways and connections.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.

   The following information is displayed:

Interconnect Gateways	• Total number of interconnect gateways • Number of interconnect gateways that reachable (Up) • Number of interconnect gateways that are unreachable (Down)
Connections	• Total number of connections • Number of connections in the Up state • Number of connections in the Down state
Summary Table	Summarized list of all interconnect gateways and connections from the gateways.
Device Link	• Total number of Device Link • Number of Device Link in the Up state • Number of Device Link in the Down state

View, Edit or Delete Connections

Note

- When you delete a connection to AWS, Cisco SD-WAN Manager deletes only the VIF, the virtual private gateway, and the route table that were created while establishing the connection.
- While creating a connection to AWS, if you created a direct connect gateway or transit gateway from Cisco SD-WAN Manager, deleting the connection does not delete the gateway. You need to manage these AWS resources as required.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you have the option to delete the Direct Connect Gateway or Transit Gateway while deleting the connection.
- When deleting a connection to AWS, because of uncommon timing issues in the order in which the resources are torn down by AWS and Equinix, it is possible that Cisco SD-WAN Manager returns an error stating a failure in connection deletion with a 400 error returned by the service provider. Cisco SD-WAN Manager fully clears the connection from its database, and clears all related device configurations. It is recommended that you login to the Equinix portal and verify that the interface configuration and association has been deleted from the Equinix database as well, so that the same interface can be reused at a later time for a different connection.

  Failure to verify the status of the interface in Equinix portal might lead to errors in creating any new connection for the same device.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

   Existing connections are summarized in a table.
4. In the table, find the desired connection and click **...**.
   - To view more information about a connection, click **View**.
   - To delete a connection, click **Delete** and confirm that you wish to delete the connection.

Edit Connection Configuration

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1 and Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Interconnect Connectivity**.

   Existing connections are summarized in a table.
4. To modify connection configuration, click **...** for the desired connection and click **Edit**.

   The following tables describe the editable parameters based on the connection destination and the connection type, if any. Configure the parameters as required.

Along with these editable parameters, Cisco Catalyst SD-WAN Manager also displays read-only properties about the connection.

Note You can modify the properties of active connections only.

Table 89: Editable Properties of Interconnect Connections to AWS

Field	Description	Applicable Connection Types
Segment	Choose a different segment ID for this connection.	All connections to AWS
Transit Gateway	**a.** Click the **Refresh** button to fetch the transit gateways associated with the selected AWS account. **b.** Choose the transit gateway to which the direct connect connection must be created. **Note** • The transit gateway that you wish to remove is not the only transit gateway associated with the connection. • You can remove VPC tags corresponding to the region served by the transit gateway in the same edit operation. **Note** You cannot replace an existing transit gateway for a region with another transit gateway from the same region.	Transit-hosted connections
VPC Tags	Choose VPC tags to identify VPCs for which traffic must be routed through this connection.	• Private-hosted connections with VPC attachments • Transit-hosted connections
Allowed Prefixes	Click **Edit Prefixes**. Enter the IPv4 Classless Inter-Domain Routing (CIDR) prefixes for the selected VPCs. You can find the IPv4 CIDR addresses from the AWS VPC Dashboard. **Note** You can add additional prefixes. You cannot remove existing prefixes.	Transit-hosted connections

Table 90: Editable Properties of Interconnect Connections to Google Cloud

Field	Description
Connection Speed	Choose the desired bandwidth from the **Connectivity Speed** drop-down list. In the case of redundant connections, modify the connection speed of either the primary or the secondary connection. The peer connection is updated to use the same connection speed. The bandwidth options for a connection may depend on the associated peering location.

Note
Modify the property of either the primary or the secondary connection. The peer connection is updated to use the same configuration.

Table 91: Editable Properties of Interconnect Connections to Microsoft Azure

Field	Description	Applicable Connection Types
Bandwidth	Modify the connection bandwidth. Unit: Mbps. **Note** You can only increase the bandwidth of connections to Microsoft Azure. For connections to Microsoft Azure, you must increase the bandwidth of the ExpressRoute on the Azure portal before increase the connection bandwidth on Cisco SD-WAN Manager.	Private and public (Microsoft) peering connections
Segment	Choose a different from segment ID for this connection.	Private and public (Microsoft) peering connections
BGP Advertise Prefix	Enter the summary addresses and prefixes you wish to advertise to the interconnect gateway. **Note** By default Microsoft Azure uses an older version of API on its portal for displaying resources or network objects that do not display the BGP advertise prefix correctly. To verify the BGP advertise prefix from the Microsoft Azure portal, select 2020-05-01 or above API version.	Public (Microsoft) peering connections
VNet Settings		
VNet	Choose VNet tags to identify the VNets for which traffic must be routed through this connection.	Private peering connections

Field	Description	Applicable Connection Types
vHub Settings	**a.** Click **Edit Settings**. **b.** Review the virtual hub name and the address-prefix for applicable regions. If a virtual hub does not exist in a region, enter the virtual hub name and address-prefix to be used for the region. **Note** Ensure that the virtual hub address-prefix that you enter does not overlap with the address-prefixes of any VNets. **c.** To apply changes, click **Save**. To discard changes, click **Cancel**.	Private peering connections

Table 92: Editable Properties of Interconnect Connections Between Edge Devices

Field	Description
Bandwidth	Modify the connection bandwidth. Unit: Mbps.

5. To apply changes, click **Update** or **Save**.

View, Edit, or Delete an Interconnect Gateway

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Click **Interconnect**.
3. Click **Gateway Management**.

   Existing interconnect gateway details are summarized in a table.
4. In the table, find the desired interconnect gateway and click **...**.
   - To view more information about the interconnect gateway, click **View**.
   - To edit the interconnect gateway description, click **Edit Interconnect Gateway**.
   - To delete the interconnect gateway, click **Delete** and confirm that you wish to delete the gateway.

     Deleting the interconnect gateway disconnects the branch location from the Equinix fabric.

View, Edit, or Delete an Interconnect Account

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.

2. Click **Interconnect**.
3. Click **Account Management**.

   The available interconnect accounts are listed in a table.
4. For the desired interconnect account, click **...** and do as follows:
   - To view more details about the interconnect account, click **View**.
   - To modify interconnect account details, click **Edit Account Information**.

     You can modify the **Account Name** and the **Description**.
   - To modify interconnect account credentials, click **Edit Account Credentials**.

     You can modify the **Customer Key** and **Customer Secret** for the account.

Note Modifying the credentials on Cisco SD-WAN Manager, does not modify the credentials with the interconnect provider. Use this configuration option only to replicate any changes to the account credentials that you have performed on the relevant portal of the Interconnect Provider.

   - To delete the interconnect account, click **Remove** and confirm that you wish to remove the account.

Audit Management

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1

The audit management support added to the fabric of the SDCI provider Equinix helps you check if the cloud state is in sync with the Cisco SD-WAN Manager state or not. The audit process involves scanning the provider resources, interconnect gateways, and connections to the cloud. When there are errors, they are displayed and if there are no errors, the status is displayed as **In Sync**.

Accessing the Audit Report

1. In the **Cloud onRamp for Multicloud** page, navigate to the **Interconnect** tab.
2. In the **Intent Management** pane, click **Audit**.
3. In the **Intent Management- Audit** screen, under **Interconnect Gateways**, choose an **Interconnect Provider** from the drop-down list.
4. Choose **Interconnect Connections**.
5. To view the desired audit report, choose a **Destination Type** and choose a **Cloud Provider** from the drop-down list when the destination type is **cloud**.
6. Select the **Device Links** option.

Parameter Name	Description
Interconnect Provider	Choose the interconnect provider type from the drop-down. The options are: • **Megaport** • **Equinix**
Interconnect Connections	Enable or disable the interconnect connections.
Destination Type	Choose the destination type from the drop-down list. The options are: • **Cloud** • **Edge**
Cloud Provider	Choose the cloud provider from the drop-down list. The options are: • **Amazon Web Servcies** • **Microsoft Azure** • **Google Cloud**
Device Links	Choose the device links for the interconnect provider.



Note After the audit is completed, the following reports are generated:

- **Edge Gateway**: Provides information about configured edge gateways.
- **Edge Connections**: Provides information about configured edge connections.
- **Unknown Edge Gateways**: Provides information about unknown edge gateways.
- **Unknown Edge Connections**: Provides information about unknown edge connections.

The following are the statuses that are displayed in the audit report along with the details:

- **In Sync**
- **Out of Sync**
- **AUDIT_INFO**

Benefits of Audit

Audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what has been realized in the cloud. The gaps are in terms of cloud resources, connectivity, and states. When such gaps are detected, Cisco SD-WAN Manager flags such gaps and helps you take corrective action.

Troubleshoot Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

Scenario	Resolution
Unable to add Interconnect Account	• Verify that the account credentials associated with Cisco SD-WAN Manager are correct. • If you updated the credentials with interconnect provider, update the account credentials on Cisco SD-WAN Manager.
While attempting to create an interconnect gateway, the device list is empty	Verify that you have attached the Equinix template to the devices. (Recommended template: *Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02*)
While attempting to create an interconnect gateway, cannot find the desired location	Click the Refresh button to update the list of available locations.
Creation of interconnect gateway failed	**1.** Check the configuration task progress on Cisco SD-WAN Manager for any error messages. **2.** If you are using the Interconnect Global Settings, check whether the selected software image is available at the Interconnect Provider location. **3.** If the VM instance is not deployed or the IP pool is exhausted, check with the Interconnect provider.
Certificate is not installed successfully for interconnect gateway	From the Cisco SD-WAN Manager menu, click **Maintenance** > **Device Reboot**. From the **Device Reboot** page, reboot the interconnect gateway.
While creating a direct connect connection, the direct connect gateway or the transit gateway list is empty	**1.** On the AWS portal, verify that the desired direct connect gateway or transit gateway is available. **2.** Click the Refresh button to fetch the list of gateways from AWS. **3.** If a gateway is not available in AWS, create the gateway through Cisco SD-WAN Manager.
While creating a direct connect connection, host VPC tags are not listed	Verify that the host VPC tags are available and enabled for Interconnect connectivity.

Scenario	Resolution
Creation of Direct Connect connection failed	**1.** Check the configuration task progress on Cisco SD-WAN Manager for any error messages. **2.** If you are using the interconnect global settings, check whether the internal IP address pool has been exhausted. If yes, delete some connections and retry. **3.** If you are using custom settings, ensure that you haven't entered overlapping CIDR subnets for peering. **4.** Check whether you have reached any connection limits. See *Usage Notes for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix*. **5.** Verify permissions of the interconnect provider account and the AWS account.
Traffic flow issues	**1.** Ensure that the required security rules for inbound and outbound traffic are configured for the host VPC. **2.** Verify whether the virtual interface has been created and attached to the direct connect gateway. **3.** In AWS, verify whether the BGP peering status is in the UP state for the virtual interface. **4.** Verify whether the correct route table is being used as the main routing table for the host VPC and whether the necessary routes are being propagated towards the virtual private gateway or the transit gateway. **5.** Verify whether the virtual private gateway or transit gateway is attached to the direct connect gateway.
Latency issues	**1.** Verify whether the interconnect gateway location is in close proximity to the direct connect location chosen while creating the connection. **2.** Ensure that you have configured the appropriate bandwidth for the connection.
Cloud gateways are not displayed in the drop-down list	Ensure that the necessary cloud gateways are created using the multicloud workflow and the minimum requirements listed in this document are met.

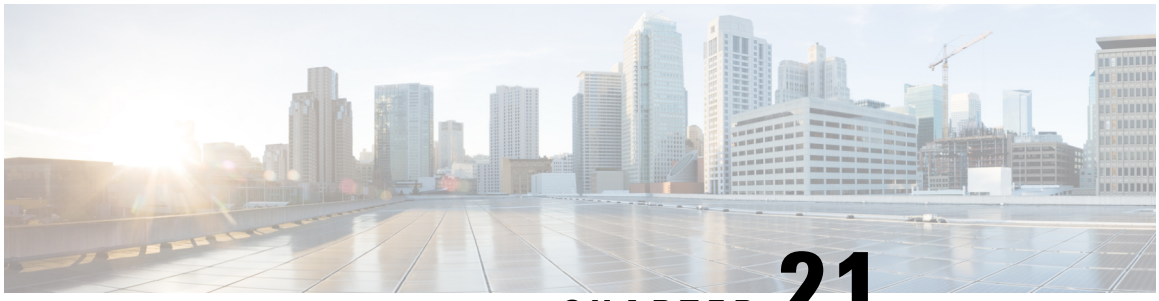
Scenario	Resolution
Traffic to VPC or VNET workload is sent over the internet even after creating an interconnect connection to the cloud gateway	When an Cisco Catalyst SD-WAN branch is connected to a cloud gateway through the internet and through an interconnect connection from an interconnect gateway to access the same VPC or VNET workload, by default, traffic from the branch is sent through the internet. To make the private path through the interconnect gateway the preferred path, apply appropriate control and data policies to the WAN edge device at the branch, the interconnect gateway, and the cloud gateway.



PART V

Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp

- Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp, on page 561



CHAPTER 21

Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp

- Overview, on page 561
- Support Articles, on page 561
- Feedback Request, on page 562
- Disclaimer and Caution, on page 562

Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following are the support articles associated with this technology:

Document	Description
Configure Azure Express Route as Transport with SD-WAN in a Click	This document describes how to integrate Express Route as an SD-WAN transport inside of the VHUB with the Cloud OnRamp for the Multi-Cloud Azure solution.

Document	Description
Configure Google Cloud Interconnect as a Transport with Cisco SD-WAN in a Click	This document describes how to use Google Cloud Interconnect as Software-Defined Wide Area Network (SD-WAN) transport.
Configure SD-WAN Cloud OnRamp for SaaS	This document describes the configuration for Cloud OnRamp for Software as a Service (SaaS) using branch local exit.

Feedback Request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the **Feedback** button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

Disclaimer and Caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.