

Cisco Catalyst SD-WAN Getting Started Guide

First Published: 2019-04-25

Last Modified: 2026-07-07

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)

© 2019–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

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

CHAPTER 3 **The Cisco Catalyst SD-WAN Solution** 5

- The Cisco Catalyst SD-WAN Solution 5
- Cisco Catalyst SD-WAN Solution 5
  - The Need for Cisco Catalyst SD-WAN Solution 5
    - Challenges in Legacy Network Design 6
    - Cisco Catalyst SD-WAN Solution 6
  - The Virtual IP Fabric 8
- Cisco Catalyst SD-WAN Components 13
  - Primary Cisco Catalyst SD-WAN Components 13
    - Cisco Catalyst SD-WAN Manager 14
    - Cisco Catalyst SD-WAN Controller 15
    - Cisco Catalyst SD-WAN Validator 16
  - Cisco vEdge Devices and Cisco IOS XE Catalyst SD-WAN Devices 17
  - Cisco Catalyst SD-WAN Control Connections 19
    - Information About Cisco Catalyst SD-WAN Control Connections 19
    - Benefits of TLS 1.3 in Cisco Catalyst SD-WAN Control Connections 20
    - Verify Cisco Catalyst SD-WAN Control Connections 20
  - Cisco Catalyst SD-WAN Solution 23
    - Cloud onRamp for SaaS 23
    - Cisco Catalyst SD-WAN Analytics 24
    - Cisco Catalyst SD-WAN Portal 24
  - Cisco SD-AVC 25

Work with Cisco Catalyst SD-WAN 25
Build a Basic Overlay Network using Cisco vEdge Devices 25
Cisco Catalyst SD-WAN Terminology 29
Domain ID 30
OMP Routes 30
Site ID 31
System IP Address 31
TLOC 31
Additional Information 31

CHAPTER 4 **Hardware and Software Installation** 33
Server Recommendations 33
Device Configuration Reset of Cisco IOS XE Catalyst SD-WAN devices after Adding or Removing Modules 34
On-Site Bootstrap Process for Cisco Catalyst SD-WAN Devices 34
On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates 37
Generate a Bootstrap File For Cisco IOS XE Catalyst SD-WAN Devices Using the CLI 42
One Touch Provisioning: Onboard Cisco IOS XE Catalyst SD-WAN Devices Using Generic Bootstrap Configuration 44
Software Installation and Upgrade for Cisco IOS XE Routers 48
Before You Begin 48
Download Cisco IOS XE Catalyst SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier 50
Install the Cisco IOS XE Catalyst SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier 50
Configure IOS XE Router Using CLI 53
Add IOS XE Devices to the Plug and Play Portal 55
Upgrading or Downgrading ROMMON 55
Perform Factory Reset 56
Recover the Default Password 57
Software Installation and Upgrade for vEdge Routers 58
Software Image Signing 58
Software Version Compatibility 58
Install the Software 59
Upgrade the Software 59

Best Practices for Software Upgrades 60
Obtain Software Images from Cisco Catalyst SD-WAN 61
Add New Software Images to the Repository 62
Upgrade the Software Image 63
Activate a New Software Image 64
View Log of Software Upgrade Activities 64
Upgrade a Software Image from the CLI 64
Redundant Software Images 65
Downgrade a Cisco vEdge Device to an Older Software Image 65
Upgrade Memory and vCPU Resources on a Virtual Machine Hosting Cisco Catalyst SD-WAN Manager 66
Expand the secondary disk size, Cisco Catalyst SD-WAN Manager Release 20.12.x and later 68
Software Maintenance Upgrade for Cisco IOS XE Catalyst SD-WAN Devices 69
Information About Software Maintenance Upgrade 69
Supported Devices for Software Maintenance Upgrade 70
Manage Software Maintenance Upgrade Images 71
Manage Software Maintenance Upgrade Images Using the CLI 72
Verify Status of Software Maintenance Upgrade Images 74

CHAPTER 5 **Cisco SD-AVC 77**
Cisco SD-AVC feature history 77
Cisco SD-AVC 77
Cloud-hosted SD-AVC service 78
Supported solutions for the cloud-hosted SD-AVC service 78
Restrictions for the cloud-hosted SD-AVC service 78
Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later 79
Enable Cisco SD-AVC, Cisco vManage Release 20.3.1 through SD-WAN Manager 20.16.x 79
Enable SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices 80
Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier 81
Enabling SD-AVC on Cisco SD-WAN Manager 82
Enable SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices 83

CHAPTER 6 **Cisco SD-AVC Cloud Connector 85**
Cisco SD-AVC Cloud Connector feature history 85

Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later 86
Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x 87
Enable Cloud Services 92

CHAPTER 7 **Install and Upgrade for Cisco Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later** 95
Install and Upgrade Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later 96
Platforms Supported in Controller Mode 96
Cisco IOS XE Image Compatibility 97
Upgrade Considerations 98
Restrictions 99
Self-Signed Trustpoint 100
Introducing Autonomous and Controller Mode 100
Software Installation for Cisco IOS XE Routers 101
Download the Software for Cisco IOS XE Release 17.2.1r or Later 101
Install Software on Cisco ASR, Cisco ISR and Cisco ENCS Platforms 101
Install Software on Cisco CSR 1000v Platform 101
Install a Cisco Catalyst 8000V Edge Software Platform 102
Plug and Play in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later Releases 103
Plug and Play Onboarding Workflow 103
Mode Discovery with Plug and Play Onboarding 104
Automatic IP Address Detection 105
Non-PnP Onboarding 106
Creating a Cisco Catalyst SD-WAN Bootstrap Configuration File 106
New Installation: Mode Change Device Day Zero Scenario 106
Switch Modes Using Cisco CLI 107
Change a device to Controller mode 108
Mode Discovery and Mode Change with Bootstrap Files 109
Reset Controller Mode Configuration 111
Mode Switching: Additional Information 113
Configuration Persistence During Mode Switch 113
Verify Controller and Autonomous Modes 113
Show Command Output for Controller Mode 113

Show Command Output for Autonomous Mode 114
Change the Console Port Access After Installation, in Controller Mode 114
Upgrade to Cisco IOS XE Release 17.2.1r or Later 116
Supported Upgrades 116
Upgrade Using Cisco Catalyst SD-WAN 118
Upgrade Using CLI 118
Downgrade from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or Later Releases 120
Downgrade a Cisco IOS XE Catalyst SD-WAN Device to a Previously Installed Software Image 120
Downgrade a Cisco IOS XE Catalyst SD-WAN Device to an Older Software Image 120
Downgrade Scenarios for Cisco IOS XE Release 17.2.x 121
Restore Smart Licensing and Smart License Reservation 122
Restore Smart Licensing 122
Restore Smart License Reservation 122
Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing 122
Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices 124
Troubleshooting 125
Troubleshooting Software Installation 125
Router Loads the Previous Software Version After Booting 125

CHAPTER 8 **Cisco Catalyst SD-WAN Overlay Network Bring-Up Process** 127
Network Overlay Bringup 127
Cisco SD-WAN Manager Persona and Storage Device 128
Bring-Up Sequence of Events 129
Steps to Bring Up the Overlay Network 131
Summary of the User Portion of the Bring-Up Sequence 134
Automatic Portions of the Bring-Up Sequence 137
User Input Required for the ZTP Automatic Authentication Process 137
Authentication between Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Validator 138
Authentication Between Cisco Catalyst SD-WAN Controllers 141
Authentication between Cisco Catalyst SD-WAN Validator and a Cisco vEdge Router 144
Authentication between the Cisco vEdge Router and Cisco SD-WAN Manager 147
Authentication between Cisco Catalyst SD-WAN Controller and the Cisco vEdge Router 149
Firewall Ports for Cisco Catalyst SD-WAN Deployments 153

Cisco Catalyst SD-WAN-Specific Port Terminology 153
Port Offset 153
Port Hopping 153
Effects of Port Hopping 155
Ports Used by Cisco vEdge Devices 155
Ports Used by Cisco Catalyst SD-WAN Devices Running Multiple vCPUs 156
Administrative Ports Used by Cisco SD-WAN Manager 157
Configure the Port Offset 158
Perform Port Hopping Manually 159
Download Software 159
Deploy Cisco SD-WAN Manager 160
Create Cisco Catalyst SD-WAN Manager VM Instance on ESXi 161
Launch vSphere Client and Create Cisco Catalyst SD-WAN Manager VM Instance 161
Create a New Virtual Disk 162
Add Additional vNICs 162
Connect Cisco Catalyst SD-WAN Manager VM Instance to Cisco Catalyst SD-WAN Manager Console 163
Create Cisco Catalyst SD-WAN Manager VM Instance on KVM 164
Create Cisco Catalyst SD-WAN Manager VM Instance on the KVM Hypervisor 164
Connect to a Cisco Catalyst SD-WAN Manager Instance 165
Configure Cisco Catalyst SD-WAN Manager 166
Configure Certificate Settings 169
Generate Cisco Catalyst SD-WAN Manager Certificate 169
Create a Cisco Catalyst SD-WAN Manager Cluster 169
Enable Timeout Value for a Cisco SD-WAN Manager Client Session 170
Deploy Cisco Catalyst SD-WAN Validator 170
Create Cisco Catalyst SD-WAN Validator VM Instance on ESXi 171
Launch vSphere Client and Create a Cisco Catalyst SD-WAN Validator VM Instance 171
Add a vNIC for the Tunnel Interface 172
Start the Cisco Catalyst SD-WAN Validator VM Instance and Connect to the Console 172
Create Cisco Catalyst SD-WAN Validator VM Instance on KVM 172
Configure Cisco Catalyst SD-WAN Validator 173
Create Configuration Templates for Cisco Catalyst SD-WAN Validator 177
Configuration Prerequisites 177

Feature Templates for Cisco Catalyst SD-WAN Validators 178
Create Feature Templates 178
Create Device Templates 179
Attach Device Templates To Cisco Catalyst SD-WAN Validator 180
Add Cisco Catalyst SD-WAN Validator to the Overlay Network 181
Start the Enterprise ZTP Server 181
Requirements for ZTP 182
Configure a Router to be a ZTP Server 184
vContainer Host 186
Deploy Cisco Catalyst SD-WAN Controller 186
Create Cisco Catalyst SD-WAN Controller VM Instance on ESXi 186
Launch vSphere Client and Create a Cisco Catalyst SD-WAN Controller VM Instance 187
Add a vNIC for the Management Interface 187
Start the Cisco Catalyst SD-WAN Controller VM Instance and Connect to the Console 188
Create Cisco Catalyst SD-WAN Controller VM Instance on KVM 188
Configure the Cisco Catalyst SD-WAN Controller 189
Create Configuration Templates for Cisco Catalyst SD-WAN Controller 194
Configuration Prerequisites 194
Feature Templates for Cisco Catalyst SD-WAN Controller 194
Create Feature Templates 195
Create Device Templates 196
Attach a Device Template To Cisco SD-WAN Controllers 197
Add Cisco Catalyst SD-WAN Controller to the Overlay Network 198
Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals 199
Notes and Limitations 199
Deploy Cisco CSR 1000v Using Cloud Service Provider Portals 199
Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud 200
Features 200
Requirements for the Cisco Catalyst 8000V Instance 200
Configure the Cisco Catalyst 8000V Instance to Connect to Cisco Catalyst SD-WAN 200
Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco Catalyst SD-WAN 201
Deploy the vEdge Cloud routers 201
Create vEdge Cloud router VM Instance on AWS 202
Create vEdge Cloud router VM Instance on Azure 207

Create vEdge Cloud VM Instance on ESXi 210
Create vEdge Cloud VM Instance on KVM 213
Configure Certificate Authorization Settings for WAN Edge Routers 215
Install Signed Certificates on vEdge Cloud Routers 216
Send Router Serial Numbers to the Controller Devices 223
How to Upload a Router Authorized Serial Number File 224
Configure the vEdge Routers 227
Enable Data Stream Collection from a WAN Edge Router 235
Prepare Routers for ZTP 236

CHAPTER 9 **Add SD-WAN Controller and SD-WAN Validator Components** 241
Add SD-WAN Controller and SD-WAN Validator components feature history 241
Add SD-WAN Controller and SD-WAN Validator components 241
Supported solutions for the Add SD-WAN Controller and SD-WAN Validator workflow 242
Supported environments for the Add SD-WAN Controller and SD-WAN Validator components workflow 242
Prerequisites for the Add SD-WAN Controller and SD-WAN Validator components workflow 242
Add SD-WAN Controllers or SD-WAN Validators using a workflow 242

CHAPTER 10 **First Time Settings on Cisco SD-WAN Manager** 245
First time settings on Cisco SD-WAN Manager 245
First time settings on Cisco SD-WAN Manager 246
Standard setup 246
Express setup 247
Enable multitenancy on Cisco SD-WAN Manager 247
Configure organization name 248
Configure common control component network settings 248
Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier 258
Configure cloud services 258
Configure certificate settings 259
Add Cisco SD-WAN Controller and Cisco SD-WAN Validator 265
Configure Cisco SD-WAN Validator IP address 265
Configure identity provider settings 265
Configure users and access 266

Alarm notification settings 267
Configure account lockout settings 268
Web server certificate for Cisco SD-WAN Manager 269

CHAPTER 11 Control Components Settings on Cisco SD-WAN Manager 271
Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager 271
Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager 271
Common Control Component Network Settings 272
Configure device specific control component network settings 282

CHAPTER 12 Cisco SD-WAN Manager Tools 289
Cisco SD-WAN Manager header 289

CHAPTER 13 Cisco services registration 293
Authentication for Cisco services 293
Restrictions for authenticating Cisco services 293
Authenticate Cisco services 294

CHAPTER 14 Quick Connect Workflow 295
Quick Connect Workflow 295
Prerequisites for Using the Quick Connect Workflow 296
Restrictions for Quick Connect Workflow 296
Information About Quick Connect 297
Overview of the Quick Connect workflow 297
Upload devices using Auto Sync 297
Upload devices manually 298
Smart Account and Virtual Account credentials 299
Access the Quick Connect Workflow 299

CHAPTER 15 Cluster Management 301
Cluster Management 301
Information About Cluster Management 302
Restrictions for cluster management 302

Manage the configuration database backup for a Cisco SD-WAN Manager cluster using the CLI 303
Guidelines for a Cisco Catalyst SD-WAN Manager Cluster 304
View Available Cluster Services 305
Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server 305
Add a Cisco Catalyst SD-WAN Manager Server to a Cluster 307
View Cisco Catalyst SD-WAN Manager Service Details 310
Edit Cisco Catalyst SD-WAN Manager Parameters 311
Update Configuration Database Login 311
Downgrade Cisco Catalyst SD-WAN Manager 313
Upgrade a Cisco SD-WAN Manager Cluster 313
Information About Cluster Upgrade 314
Prerequisites for Cluster Upgrade 315
Upgrade cluster software using SD-WAN Manager 316
Upgrade a Cluster Using CLI 317
Manually Restart Cisco Catalyst SD-WAN Manager Processes 319
Remove Cisco Catalyst SD-WAN Manager Nodes from a Cluster 321

CHAPTER 16 **Automated Certificate Management** 323
Feature history for automated certificate management 323
Automated certificate management 323
Prerequisites for automated certificate management on CA servers 324
Configure certificate settings 325
Troubleshoot certificate management on CA server 331

CHAPTER 17 **Certificate Management** 333
Feature history 333
Manage Certificates in Cisco Catalyst SD-WAN Manager 334
Check the WAN Edge Router Certificate Status 335
Validate a WAN Edge Router 335
Stage a WAN Edge Router 335
Invalidate a WAN Edge Router 336
Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator 336
Install Signed Certificate 337
Export Root Certificate 337

View a Certificate Signing Request 338
View a Device Certificate Signing Request 338
View the Certificate 338
Generate a Certificate Signing Request 339
Generate a controller certificate signing request, through SD-WAN Manager 20.16.x 339
Generate a feature certificate signing request, through SD-WAN Manager 20.16.x 339
Generate a WAN edge device certificate signing request, through SD-WAN Manager 20.16.x 340
Reset the RSA Key Pair 340
Invalidate a Control Component 340
View Log of Certificate Activities 341
View a Signed Certificate 341
Certificate Revocation 341
Information About Certificate Revocation 342
Restrictions for Certificate Revocation 342
Configure Certificate Revocation 342
Cisco PKI Certificates 343
Cisco PKI Certificates 343
Renew a Certificate 344
How Cisco SD-WAN Manager installs a new certificate on an edge device 345
Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices Using Cisco SD-WAN Manager 345
Information About Configure CA Certificates Using Cisco SD-WAN Manager 346
Supported Devices for Uploading CA Certificates 346
Prerequisites to Configuring CA Certificates 346
Restrictions for Uploading CA Certificates 346
Upload CA Certificates 347
Configure CA Certificates Using Cisco SD-WAN Manager 347
Revoke the CA Certificates 348
Renew the CA Certificates 349
Monitor CA Certificates and PKI Trustpoints 349
CRL-Based Quarantine 350
Information About CRL-Based Quarantine 350
Restrictions for CRL-Based Quarantine 351
Configure CRL-Based Quarantine 351

Manage Root Certificate Authority Certificates in Cisco Catalyst SD-WAN Manager 352
Add a Root Certificate Authority Certificate 352
View a Root Certificate Authority Certificate 352
Delete a Root Certificate 353
Enterprise Certificates 353
Configure Enterprise Certificates for Cisco SD-WAN Controllers 354
Information About Enterprise Certificates 355
Dependency on OU Fields in Enterprise Certificates 356
Devices that Support Enterprise Certificates 356
Configure Enterprise Certificates 356
Invalidate a Device Certificate 359
Authorize a Controller Certificate for an Enterprise Root Certificate 359
Generate a Bootstrap Configuration 361
Cisco PKI Controller Certificates 361
Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above 362
Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal 364
Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers 367
Web Server Certificate for Cisco SD-WAN Manager 368

CHAPTER 18 **Cisco SD-WAN Control Components Certificate Management 371**
SD-WAN Control Components certificate management feature history 371
Control Components Certificate Management workflow 371
Supported environments for the Control Components Certificate Management workflow 372
Supported components for the Control Components Certificate Management workflow 372
Renew Certificates using the Control Components Certificate Management workflow 372

CHAPTER 19 **Edge device certificate management 375**
Edge device certificate management feature history 375
Edge device certificate management 376
Edge device certificate management feature history 376
WAN edge device certificate management workflow 376
Supported components for the edge device certificate management workflow 376
Supported solutions for the edge device certificate management workflow 376

Renew certificates using the edge device certificate management workflow 377

CHAPTER 20 **Expired Enterprise Certificate Indication and Quarantine** 379

Expired Certificate Indication and Quarantine 379

Information About Expired Certificate Indication and Quarantine 379

Enable Quarantining Devices with Expired Certificates 381

View and Remedy Devices in Expired Certificate Quarantine 381

CHAPTER 21 **Reverse Proxy** 383

Reverse Proxy 383

Information About Reverse Proxy 383

Support for a Device with Both Private Network and Public Internet Connectivity 384

Restrictions for Reverse Proxy 385

Provision Certificates on the Reverse Proxy 386

Configure Reverse Proxy Using Cisco SD-WAN Manager 387

Configure Reverse Proxy Settings 387

Configure Reverse Proxy Settings on Cisco SD-WAN Controllers 387

Disable Reverse Proxy 389

Monitor Reverse Proxy Using CLI 389

Monitor Reverse Proxy Using CLI 393

CHAPTER 22 **Onboarding Modular Cisco ASR 1000 Series Platforms** 397

Cisco ASR 1006-X with an RP3 Module 397

Information About the Cisco ASR 1006-X with an RP3 Module 397

Hardware Configuration 398

ROM Monitor Software Version 399

Onboarding Workflow 399

RMA Replacement of the Cisco ASR 1006-X Chassis 399

RMA Replacement of the Cisco RP3 Module 403

CHAPTER 23 **Getting started with the SD-WAN Manager API** 407

SD-WAN Manager APIs 407

CHAPTER 24 **Deploy Cisco SD-WAN Controller in Microsoft Azure** 409

Information About Deploying Cisco SD-WAN Controllers in Azure 409

Benefits of Deploying Cisco SD-WAN Controllers in Azure 410

Prerequisites for Deploying Cisco SD-WAN Controllers in Azure 410

Use Cases for Deploying Cisco SD-WAN Controllers in Azure 411

Deploy Cisco SD-WAN Controllers in Azure: Tasks 411

Task 1: Create a Controller Image in Azure 411

Task 2: Create a Virtual Network, Subnets, and Network Security Group in Azure 412

Task 3: Create a Virtual Machine for the Controller 413

Task 4: Configure the Network Security Group 416

Verify the Deployment of Cisco SD-WAN Controllers in Azure 416

Monitor the Deployment of Cisco SD-WAN Controllers in Azure 417

CHAPTER 25 **Deploy Cisco SD-WAN Controllers in the AWS Cloud** 419

Information About Deploying Cisco SD-WAN Controllers in AWS 419

Benefits of Deploying Cisco SD-WAN Controllers in AWS 420

Prerequisites for Deploying Cisco SD-WAN Controllers in AWS 421

Use Cases for Deploying Cisco SD-WAN Controllers in AWS 421

Deploy Cisco SD-WAN Controllers in AWS: Tasks 421

Task 1: Request AWS AMI Images 421

Task 2: Create a VPC, Subnet, and Security Group in AWS 422

Task 3: Create a Virtual Machine for the Controller 423

Task 4: Configure the Security Group 425

Verify the Deployment of Cisco SD-WAN Controllers in AWS 426

Monitor the Deployment of Cisco Catalyst SD-WAN Controller in AWS 426

CHAPTER 26 **Troubleshoot Cisco Catalyst SD-WAN Solution** 427

Overview 427

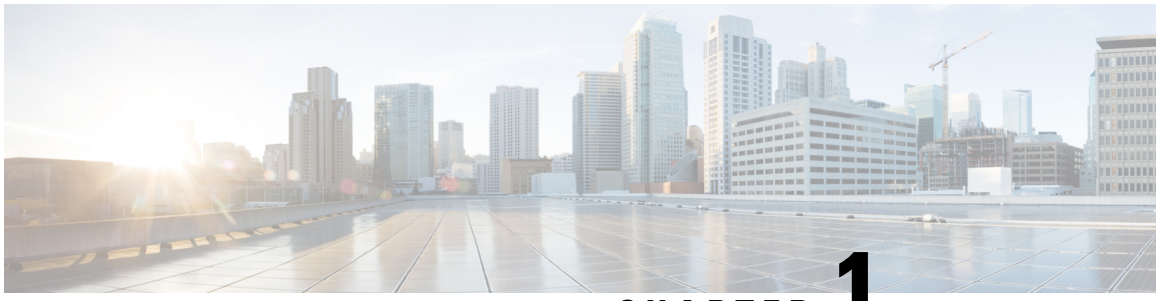
Support Articles 427

Feedback Request 429

Disclaimer and Caution 429

CHAPTER 27 **Appendix: Cisco Catalyst SD-WAN Manager How-Tos** 431

RESTful API for Cisco Catalyst SD-WAN Manager 431
Replace a vEdge Router 433
Replace a Cisco IOS XE Catalyst SD-WAN Device 435
Using Cisco Catalyst SD-WAN Manager on Different Servers 438
Log In to the Cisco Catalyst SD-WAN Manager Web Application Server 439



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
- User Documentation for Cisco SD-WAN Release 20

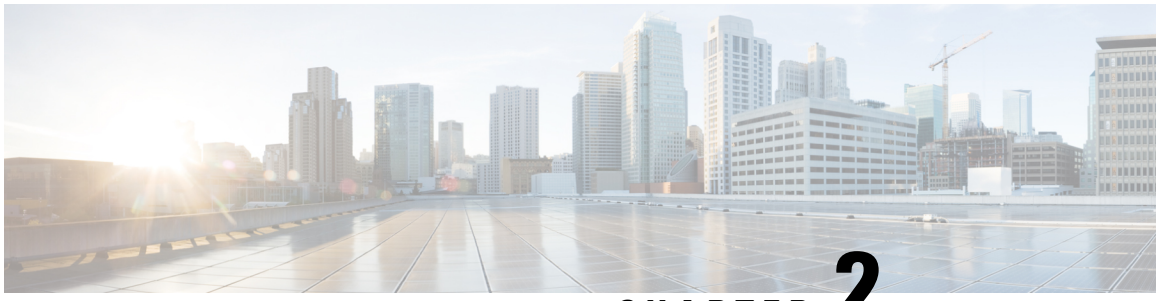
Communications, Services, and Additional Information

- 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 (SD-WAN) and Cisco Catalyst SD-WAN Releases

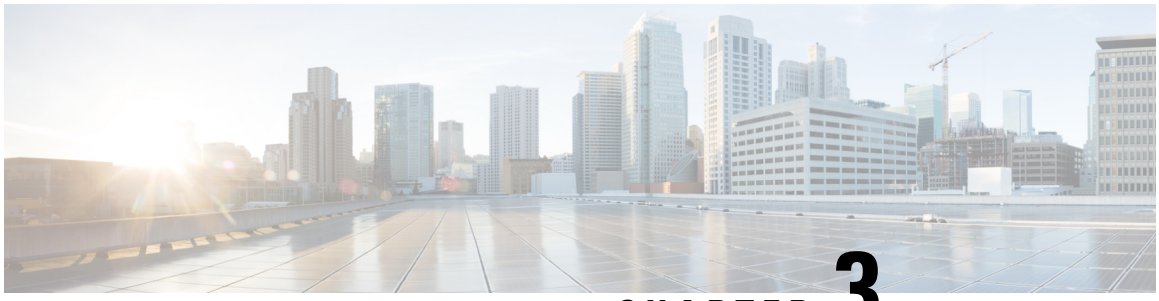
Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following links includes release-wise new and modified features that are documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

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

What's New in Cisco IOS XE Catalyst SD-WAN Release 16.x

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

What's New in Cisco SD-WAN (vEdge) Release 19.x



CHAPTER 3

The Cisco Catalyst SD-WAN Solution

- The Cisco Catalyst SD-WAN Solution, on page 5
- Cisco Catalyst SD-WAN Solution, on page 5
- Cisco Catalyst SD-WAN Components, on page 13
- Work with Cisco Catalyst SD-WAN, on page 25

The Cisco Catalyst SD-WAN Solution

Table 1: Feature History

Feature Name	Release Information	Feature Description
Support for the TLS 1.3 Protocol for Cisco Catalyst SD-WAN Control Connections	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds support for the Transport Layer Security (TLS) 1.3 protocol for Cisco Catalyst SD-WAN control connections.
Block NETCONF Requests on Cisco IOS XE Catalyst SD-WAN devices	Cisco IOS XE Catalyst SD-WAN Release 17.18.1aCisco Catalyst SD-WAN Manager Release 20.18.1	This feature introduces a security update for Cisco IOS XE Catalyst SD-WAN devices. It blocks NETCONF requests on all IP addresses except the system IP to enhance device security. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the feature blocks port 830 by default.

Cisco Catalyst SD-WAN Solution

The Need for Cisco Catalyst SD-WAN Solution

Legacy networking technology has become increasingly expensive and complex, and it cannot scale to meet the needs of today's multisite enterprises. The Cisco Catalyst SD-WAN Solution, which is based on time-tested and proven elements of networking, offers an elegant, software-based solution that reduces the costs of running enterprise networks and provides straightforward tools to simplify the provisioning and management of large

and complex networks that are distributed across multiple locations and geographies. Built in to the Cisco Catalyst SD-WAN Solution are inherent authentication and security processes that ensure the safety and privacy of the network and its data traffic.

Cisco Catalyst SD-WAN Solution represents an evolution of networking from an older, hardware-based model to a secure, software-based, virtual IP fabric. Cisco Catalyst SD-WAN fabric, also called an *overlay network*, forms a software overlay that runs over standard network transport services, including the public Internet, MPLS, and broadband. The overlay network also supports next-generation software services, thereby accelerating your shift to cloud networking.

Challenges in Legacy Network Design

The traditional approach to network design cannot scale to meet today's needs for four fundamental reasons:

- Cost: Legacy networks run on expensive hardware such as routers and switches, which require time-consuming configuration and maintenance. In addition, these networks require expensive transport connections or carrier circuits to secure and segment the network.
- Complexity: Legacy networks operate on the old model of a distributed control plane, which means that every node in the network must be configured with routing and security rules. Remote site management, change control, and network maintenance represent major logistical challenges.
- Lengthy installation times: Legacy networks that run on dedicated carrier circuits depend on the carrier to install new circuits, which can take several months. This can dramatically delay the launch of new branch locations.
- Control: Legacy networks that run on carrier circuits sacrifice control to the ISP, from network design to configuration to monitoring. Requesting changes from the ISP also requires extra time and is prone to communication errors.

Cost and complexity become even more prohibitive for legacy networks in the face of today's requirements, including:

- Rigorous end-to-end security
- Disparate transport networks
- High-bandwidth cloud applications that are hosted in multiple data centers
- Ongoing increase in the number of mobile end users
- Any-to-any connectivity over fluid topologies
- Unique needs of particular businesses

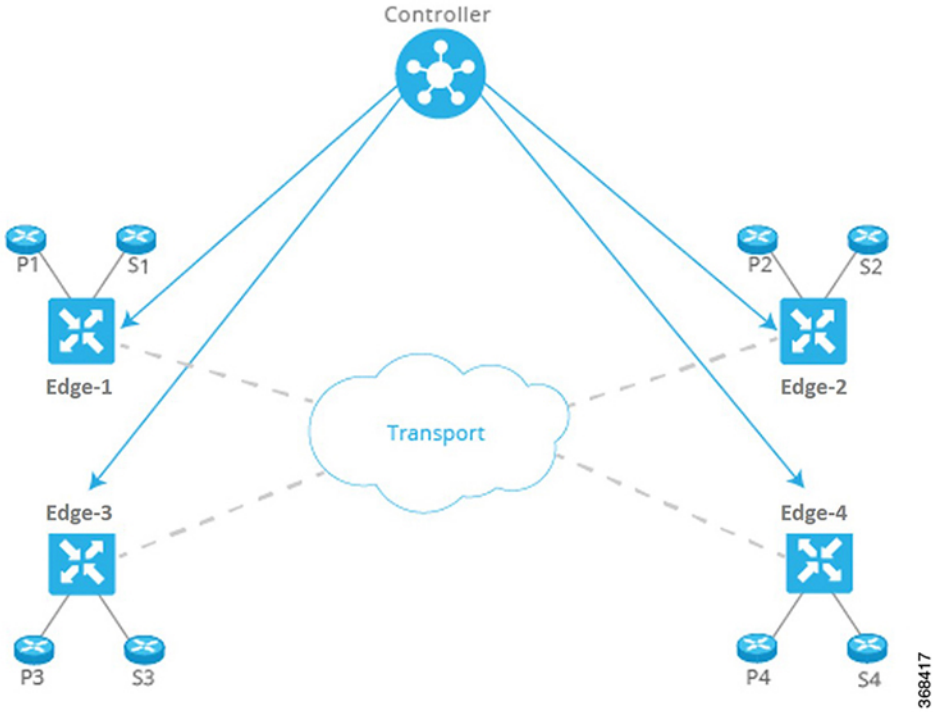
Cisco Catalyst SD-WAN Solution

The Cisco Catalyst SD-WAN solution is a Software-Defined WAN (SD-WAN). As with all SD-WANs, it is based on the same routing principles that allowed the Internet to scale during the 1990s and 2000s. What separates Cisco Catalyst SD-WAN from other SD-WANs is that it reimagines the WAN for a new generation of enterprise networks, separating the data plane from the control plane and virtualizing much of the routing that used to require dedicated hardware.

The virtualized network runs as an overlay on cost-effective hardware, whether physical routers or virtual devices. Centralized controllers, called SD-WAN Controllers, oversee the control plane of the fabric, efficiently managing provisioning, maintenance, and security for the entire Cisco Catalyst SD-WAN overlay network.

Another device, called the Cisco SD-WAN Validator, automatically authenticates all other Cisco vEdge devices when they join the Cisco Catalyst SD-WAN overlay network.

Figure 1: Components of the Cisco Catalyst SD-WAN Solution



This division of labor allows each networking layer to focus on what it does best. The control plane manages the rules for the routing traffic through the overlay network, and the data plane passes the actual data packets among the network devices. The control plane and data plane form the warp and weft of a flexible, robust fabric that you weave according to your needs, on your schedule, over existing circuits.

Cisco SD-WAN Manager provides a simple, yet powerful, set of graphical dashboards for monitoring network performance on all devices in the overlay network, from a centralized monitoring station. In addition, Cisco SD-WAN Manager provides centralized software installation, upgrade, and provisioning, whether for a single device or as a bulk operation for many devices simultaneously.

Cisco Catalyst SD-WAN is ideally suited to the needs of cloud networking. Cisco Catalyst SD-WAN virtual IP fabric supports software services that streamline and optimize cloud networking, allowing you to take full advantage of the power of the overlay network for individual cloud applications.

Note

- Cisco SD-WAN Controllers are purpose-built, custom stacks. Although open-source Linux components are used, our custom operating system stacks bear no resemblance to the open-source Linux components used. The Linux components are not subject to the same hardening requirements as the custom operating system stacks that they are used in.
- The root access is disabled on Cisco SD-WAN Controllers and cannot be accessed from the user space.
- We meet compliance standards and requirements, such as, FedRAMP, FIPS, and CC. This compliance should be considered as proof of the security validation of our operating systems.
- We follow a secure development lifecycle outlined here.
- We also follow a well-defined process run by the Cisco Product Security Incident Response Team (PSIRT) to address any new exploits or attacks, such as, CVE.
- If you are still concerned about the platform security of Cisco SD-WAN Controllers, we recommend that you conduct an independent penetration testing through third parties.

The Virtual IP Fabric

The complexity in legacy enterprise networks stems from three main sources:

- There is no clear separation between entities that exchange data traffic and the transport network that binds these entities together. That is, there is no clear separation between hosts, devices, and servers on the service side of the network and the interconnects between routers on the transport side of the network.
- Policy and control decisions are embedded at every hop across the enterprise network.
- Security is a time-intensive, manual process, and security management must be implemented either at every node in the network or by using centralized security servers to manage group keys.

Cisco Catalyst SD-WAN uses time-tested and proven elements of networking in innovative ways to build the secure, virtual IP fabric. These networking elements include:

- Using routing and routing advertisements to establish and maintain the flow of traffic throughout the network.
- Layer 3 segmentation, sometimes called virtual routing and forwarding (VRF), to isolate different flows of traffic. This is useful to separate traffic from different customers or different business organizations within an enterprise.
- Peer-to-peer concepts to set up and maintain bidirectional connections between pairs of protocol entities
- Authentication and encryptions
- Policies for routing and data traffic

With five simple steps, Cisco Catalyst SD-WAN virtual IP fabric transforms a complex legacy network into an easy-to-manage, scalable network:

- Step 1: Separate transport from the service side of the network
- Step 2: Centralize routing intelligence and enable segmentation

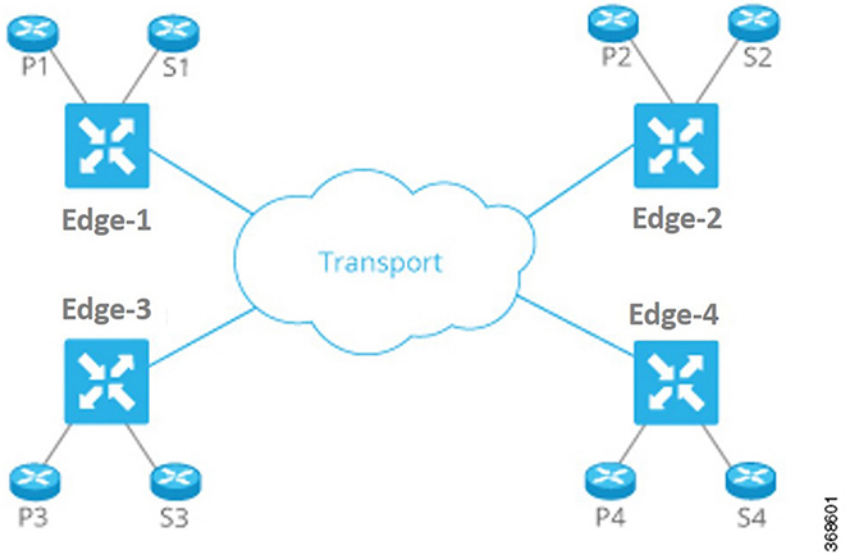
- Step 3: Secure the network automatically
- Step 4: Influence reachability through centralized policy
- Step 5: Simplify orchestration and provisioning

Step 1: Separate Transport from the Service Side of the Network

The job of the transport network is to carry packets from one transport router to another. The transport network needs to know only about the routes to follow to reach the next-hop or destination router. It need not know about the prefixes for nontransport routers, the routers that sit behind the transport routers in their local service networks.

Separating network transport from the service side of the network allows the network administrator to influence router-to-router communication independently of the communication between users or between hosts.

Figure 2: Transport Network Separated from Service Network



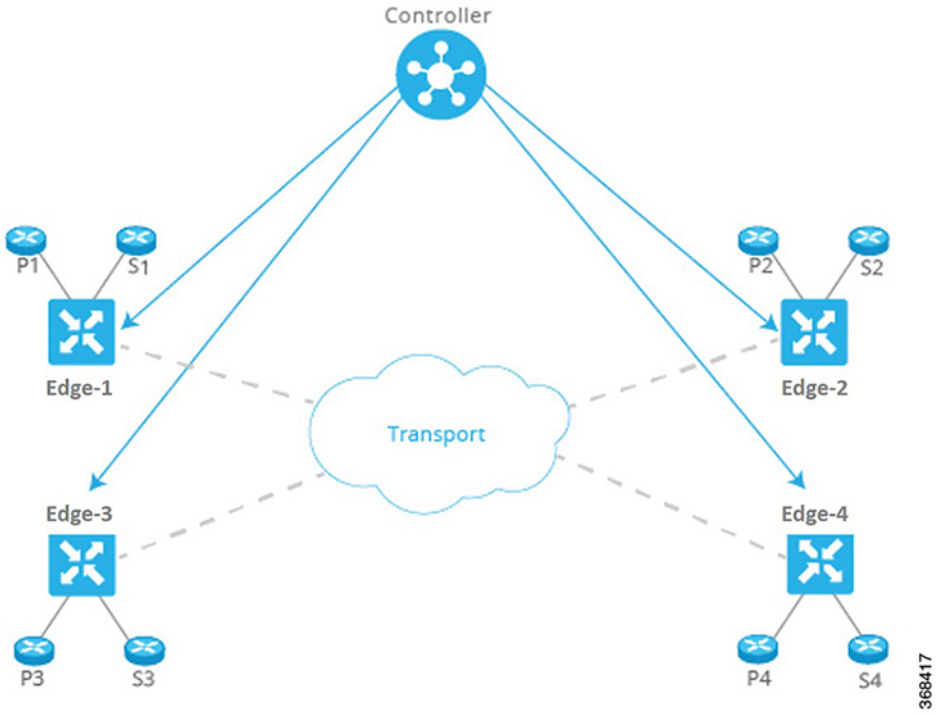
This approach has many benefits:

- The network administrator can choose transport circuits based on SLA and cost.
- The routing system can assign attributes to transport links for optimal routing, load balancing, and policy-based routing.

Step 2: Centralize Routing Intelligence and Enable Segmentation

Every router at the edge of a network has two sides for routing: one to the transport network and one to the service side of the network. To have any-to-any communication among all routers, all routers need to learn all prefixes. Traditionally, routers learn these prefixes using full-mesh IGP/BGP or by enabling routing on an overlay tunnel (for example, BGP or IGP over MPLS or GRE). Various techniques allow the scaling issues associated with full-mesh routing adjacencies to be mitigated or eliminated, such as employing a route reflector for BGP.

Figure 3: Centralizing Routing Intelligence with a Centralized Controller



The Cisco Catalyst SD-WAN fabric builds on the route reflector model by centralizing routing intelligence. Essentially, all prefixes learned from the service side on a router are advertised to a centralized controller, which then reflects the information to other routers over the network's control plane. The controllers do not handle any of the data traffic; they are involved only in control plane communication.

This approach has many benefits:

- The centralized controller can use inexpensive or commodity servers for control plane processing.
- The routers can use off-the-shelf silicon, allowing cost benefits from economies of scale.
- Scale challenges associated with full-mesh routing on the transport side of the network are eliminated.
- The network administrator can create multiple segments without the need for complex signaling protocols. For example, in the figure here, all Px prefixes can be part of one VPN, while all Sx prefixes can be part of a different VPN.

Note The centralized controller only "influences" routing on the routers. The controller does not participate in every flow going through the network, nor does it participate in routing on the service side. This design allows the routers to have local intelligence—enough intelligence to make local site decisions quickly.

Step 3: Secure the Network and Links Automatically

The Cisco Catalyst SD-WAN fabric identifies transport side links and automatically encrypts traffic between sites. The associated encryption keys are exchanged over a secure session with the centralized controller. Secure sessions with the controller are set up automatically using RSA and certificate infrastructure.

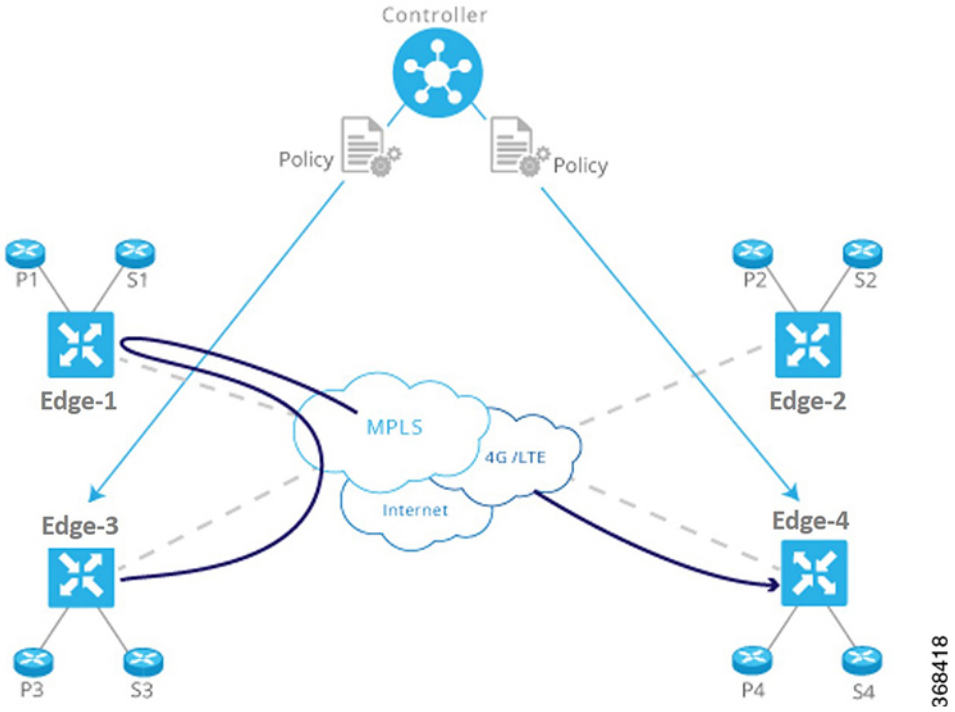
This approach has many benefits:

- The Cisco Catalyst SD-WAN fabric itself authenticates all devices participating in the network, which is an important step to secure the infrastructure.
- The fabric automatically exchanges encryption keys associated with the transport links, eliminating the hassle of configuring thousands of pair-wise keys.
- The fabric ensures that the network is not prone to attacks from the transport side.

Step 4: Influence Reachability through Centralized Policy

Policy configured on a centralized controller strongly influences how prefixes are advertised among the routers. For example, if all traffic between routers P3 and P4 in the figure here has to make a U-turn at router vEdge-1, the network administrator can apply a simple route policy on the centralized controller. The controller then passes the policy to the affected edge routers. The network administrator does not need to provision the policy on each individual router.

Figure 4: Policy Configured on a Centralized Controller



This approach has many benefits:

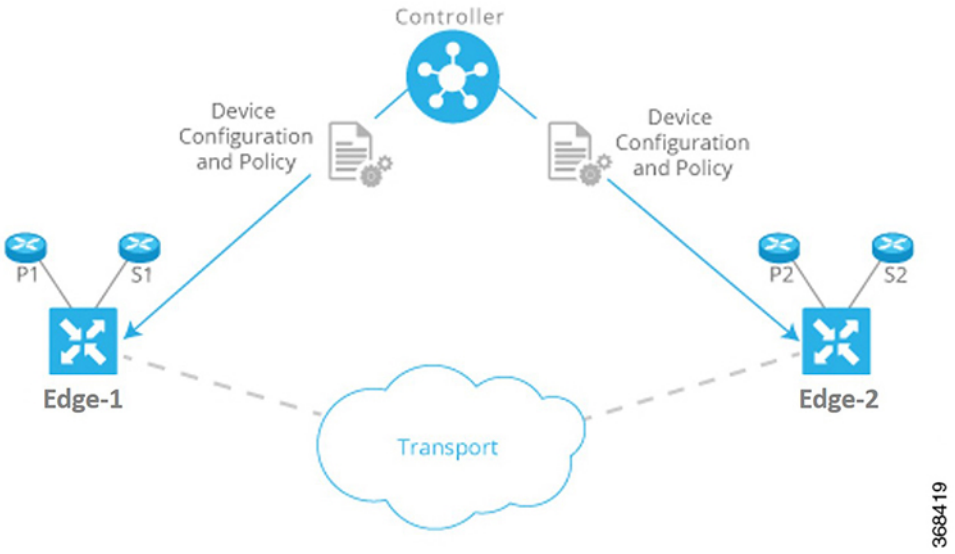
- The controller centrally influences access control, that is, which prefixes are allowed to talk to each other inside a VPN.

- The controller optimizes user experience by influencing transport link choice based on SLA or other attributes. The network administrator can color transport links (such as gold and bronze), and allow applications to map the colors to appropriate transport links.
- The network administrator can map business logic from a single centralized point.
- The network can react faster to planned and unexpected situations, such as routing all traffic from high-risk countries through an intermediate point.
- The network can centralize services such as firewalls, IDPs, and IDSs. Instead of distributing these services throughout the network at every branch and campus, the network administrator can centralize these functions, achieving efficiencies of scale and minimizing the number of touch points for provisioning.

Step 5: Simplify Provisioning and Management

Legacy network devices are provisioned and monitored manually through a CLI. Network administrators must type configurations line by line, and enter operational commands one at a time on individual devices in order to retrieve and read status information. This method is error prone and time consuming when provisioning and troubleshooting a network, and it can present serious difficulties when devices are in remote locations or when management ports are inaccessible.

Figure 5: Simplified Provisioning and Management of a Network by Cisco Catalyst SD-WAN



Cisco Catalyst SD-WAN centralizes and significantly simplifies provisioning and management through Cisco SD-WAN Manager. Cisco SD-WAN Manager provides an easy-to-use, graphical dashboard from which you can monitor, configure, and maintain all Cisco vEdge devices and links in the overlay network. For example, the GUI dashboard provides a templated view of various configurations to ease provisioning a service, so all common elements, such as AAA and company-specific servers, can be pushed to multiple devices with a single click, from a single point.

This approach has many benefits:

- The network administrator provisions and manages the network as a whole, efficiently and easily, as opposed to a piece-meal approach that deals with individual devices one at a time.

- The network administrator has improved network visibility (for example, viewing network-wide VPN statistics) from a single point.
- Troubleshooting tasks are simplified and presented visually, instead of requiring network administrators to read lengthy configurations and output from individual devices.

Cisco Catalyst SD-WAN Components

Primary Cisco Catalyst SD-WAN Components

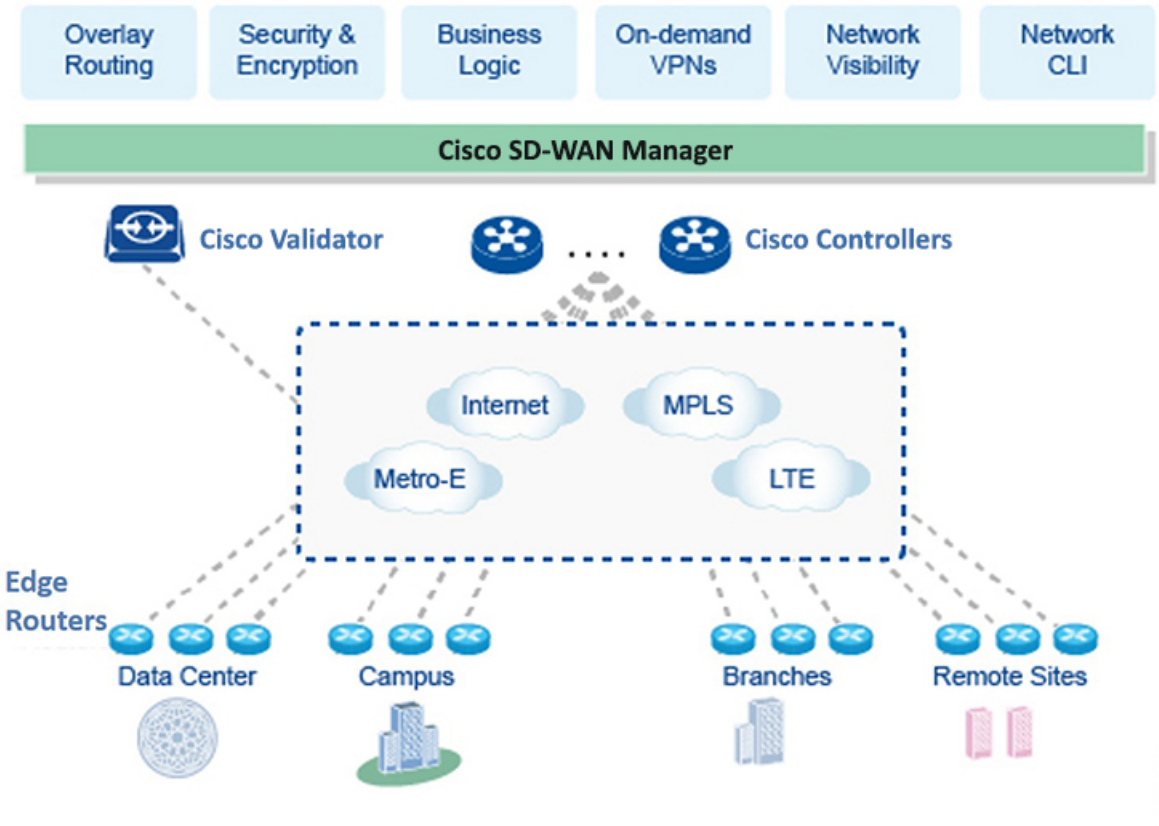
The secure, virtual IP fabric of Cisco Catalyst SD-WAN is made up of four fundamental components:

- **Cisco SD-WAN Manager**: Cisco SD-WAN Manager is a centralized network management system that lets you configure and manage the entire overlay network from a simple graphical dashboard.
- **Cisco SD-WAN Controller**: The Cisco SD-WAN Controller is the centralized brain of the Cisco Catalyst SD-WAN solution, controlling the flow of data traffic throughout the network. The Cisco SD-WAN Controller works with the Cisco SD-WAN Validator to authenticate Cisco vEdge devices as they join the network and to orchestrate connectivity among the edge routers.
- **Cisco SD-WAN Validator**: The Cisco SD-WAN Validator automatically orchestrates connectivity between edge routers and Cisco SD-WAN Controllers. If any edge router or Cisco SD-WAN Controller is behind a NAT, the Cisco SD-WAN Validator also serves as an initial NAT-traversal orchestrator.
- **Cisco IOS XE Catalyst SD-WAN and Cisco vEdge Devices**: The edge routers sit at the perimeter of a site (such as remote offices, branches, campuses, data centers) and provide connectivity among the sites. They are either hardware devices or software (Cloud router), that runs as a virtual machine. The edge routers handle the transmission of data traffic.

Of these four components, the edge router can be a Cisco Catalyst SD-WAN hardware device or software that runs as a virtual machine, and the remaining three are software-only components. The Cloud router, Cisco SD-WAN Manager, and Cisco SD-WAN Controller software runs on servers, and the Cisco SD-WAN Validator software runs as a process (daemon) on a edge router.

The figure below illustrates the components of Cisco Catalyst SD-WAN. The sections below describe each component in detail.

Figure 6: Components of Cisco Catalyst SD-WAN



Cisco Catalyst SD-WAN Manager

Cisco SD-WAN Manager is a centralized network management system. Cisco SD-WAN Manager dashboard provides a visual window into the network, and it allows you to configure and manage Cisco edge network devices. Cisco SD-WAN Manager software runs on a server in the network. This server is typically situated in a centralized location, such as a data center. It is possible for Cisco SD-WAN Manager software to run on the same physical server as Cisco SD-WAN Controller software.

You can use Cisco SD-WAN Manager to store certificate credentials, and to create and store configurations for all Cisco edge network components. As these components come online in the network, they request their certificates and configurations from Cisco SD-WAN Manager. When Cisco SD-WAN Manager receives these requests, it pushes the certificates and configurations to the Cisco edge network devices.

For Cloud routers, Cisco SD-WAN Manager can also sign certificates and generate bootstrap configurations, and it can decommission the devices.

Secure Communication with Devices and Controllers through a vmanage-admin Account

Cisco SD-WAN Manager communicates with edge devices and controllers using a secure channel—either a datagram transport layer security (DTLS) tunnel or transport layer security (TLS) tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session. It uses an internal-use-only passwordless "vmanage-admin" user account on the device or controller. The

vmanage-admin account is created during the initial device or controller setup. Cisco SD-WAN Manager uses this secure channel for monitoring, configuring, and managing each of the following:

- Edge devices
- Cisco SD-WAN Manager nodes in a cluster
- Cisco SD-WAN Validator
- Cisco SD-WAN Controllers



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1, access to port 830, which is used for NETCONF requests, is restricted. The NETCONF requests can only be sent to the Cisco IOS XE Catalyst SD-WAN device's system IP by Cisco SD-WAN Manager. This system IP serves as the main point of contact for managing and configuring the device within the network.

As noted, the vmanage-admin user accounts do not have any password associated with them, so Cisco SD-WAN Manager uses a passwordless procedure to log in to the account. To accomplish this, Cisco SD-WAN Manager generates an asymmetric encryption public-private key pair. During deployment of an edge device into the Cisco Catalyst SD-WAN fabric, or of a controller instance, Cisco SD-WAN Manager copies the public key that it has generated to the edge device or instance. It sends the public key using a proprietary protocol, within a secure channel—a DTLS or TLS tunnel.

The activity that Cisco SD-WAN Manager performs using the vmanage-admin account appears in syslog messages and in the output of certain **show** commands. The syslog messages are logged with the same level of detail as activities performed through any other user account. The level of syslog detail depends on the syslog configuration of the device.

Cisco SD-WAN Manager requires the vmanage-admin account on devices in the fabric in order to monitor, configure, and manage the devices. Removing, disabling, or altering this account on a device would prevent Cisco SD-WAN Manager from performing these activities, and is not supported.

Cisco Catalyst SD-WAN Controller

The Cisco SD-WAN Controller oversees the control plane of the Cisco Catalyst SD-WAN overlay network, establishing, adjusting, and maintaining the connections that form the Cisco Catalyst SD-WAN fabric.

The major components of the Cisco SD-WAN Controller are:

- Control plane connections: Each Cisco SD-WAN Controller establishes and maintains a control plane connection with each edge router in the overlay network. (In a network with multiple Cisco SD-WAN Controllers, a single Cisco SD-WAN Controller may have connections only to a subset of the edge routers, for load-balancing purposes.) Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco SD-WAN Controller and the edge router. This payload consists of route information necessary for the Cisco SD-WAN Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the Edge routers. The DTLS connection between a Cisco SD-WAN Controller and an edge router is a permanent connection. The Cisco SD-WAN Controller has no direct peering relationships with any devices that an edge router is connected to on the service side.
- OMP (Overlay Management Protocol): The OMP protocol is a routing protocol similar to BGP that manages the Cisco Catalyst SD-WAN overlay network. OMP runs inside DTLS control plane connections

and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the Cisco SD-WAN Controller and the edge routers and carries only control plane information. The Cisco SD-WAN Controller processes the routes and advertises reachability information learned from these routes to other edge routers in the overlay network.

- Authentication: The Cisco SD-WAN Controller has pre-installed credentials that allow it to authenticate every new edge router that comes online. These credentials ensure that only authenticated devices are allowed access to the network.
- Key reflection: The Cisco SD-WAN Controller receives data plane keys from an edge router and reflects them to other relevant edge routers that need to send data plane traffic.
- Policy engine: The Cisco SD-WAN Controller provides rich inbound and outbound policy constructs to manipulate routing information, access control, segmentation, extranets, and other network needs.
- Netconf and CLI: Netconf is a standards-based protocol used by Cisco SD-WAN Manager to provision a Cisco SD-WAN Controller. In addition, each Cisco SD-WAN Controller provides local CLI access and AAA.

The Cisco SD-WAN Controller maintains a centralized route table that stores the route information, called OMP routes, that it learns from the edge routers and from any other Cisco SD-WAN Controllers in the Cisco Catalyst SD-WAN overlay network. Based on the configured policy, the Cisco SD-WAN Controller shares this route information with the Cisco edge network devices in the network so that they can communicate with each other.

The Cisco SD-WAN Controller is a software that runs as a virtual machine on a server configured with ESXi or VMware hypervisor software. The Cisco SD-WAN Controller software image is a signed image that is downloadable from the Cisco Catalyst SD-WAN website. A single Cisco Catalyst SD-WAN root-of-trust public certificate is embedded into all Cisco SD-WAN Controller software images.

During the initial startup of a Cisco SD-WAN Controller, you enter minimal configuration information, such as the IP addresses of the controller and the Cisco SD-WAN Validator. With this information and the root-of-trust public certificate, the Cisco SD-WAN Controller authenticates itself on the network, establishes a DTLS control connection with the Cisco SD-WAN Validator, and receives and activates its full configuration from Cisco SD-WAN Manager if one is present in the domain. (Otherwise, you can manually download a configuration file or create a configuration directly on the Cisco SD-WAN Controller through a console connection.) The Cisco SD-WAN Controller is now also ready to accept connections from the edge routers in its domain.

To provide redundancy and high availability, a typical overlay network includes multiple Cisco SD-WAN Controllers in each domain. A domain can have up to 20 Cisco SD-WAN Controllers. To ensure that the OMP network routes remain synchronized, all the Cisco SD-WAN Controllers must have the same configuration for policy and OMP. However, the configuration for device-specific information, such as interface locations and addresses, system IDs, and host names, can be different. In a network with redundant Cisco SD-WAN Controllers, the Cisco SD-WAN Validator tells the Cisco SD-WAN Controllers about each other and tells each Cisco SD-WAN Controller which edge routers in the domain it should accept control connections from. (Different edge routers in the same domain connect to different Cisco SD-WAN Controllers, to provide load balancing.) If one Cisco SD-WAN Controller becomes unavailable, the other controllers automatically and immediately sustain the functioning of the overlay network.

Cisco Catalyst SD-WAN Validator

Cisco SD-WAN Validator automatically coordinates the initial bringup of Cisco SD-WAN Controllers and edge routers, and it facilities connectivity between Cisco SD-WAN Controllers and edge routers. During the

bringup processes, the Cisco SD-WAN Validator authenticates and validates the devices wishing to join the overlay network. This automatic orchestration process prevents tedious and error-prone manual bringup.

Cisco SD-WAN Validator is the only Cisco vEdge device that is located in a public address space. This design allows the Cisco SD-WAN Validator to communicate with Cisco SD-WAN Controllers and edge routers that are located behind NAT devices, and it allows the Cisco SD-WAN Validator to solve any NAT-traversal issues of these Cisco vEdge devices.

The major components of the Cisco SD-WAN Validator are:

- Control plane connection: Each Cisco SD-WAN Validator has a persistent control plane connection in the form of a DTLS tunnel with each Cisco Catalyst SD-WAN Controller in its domain. In addition, the Cisco SD-WAN Validator uses DTLS connections to communicate with edge routers when they come online, to authenticate the router, and to facilitate the router's ability to join the network. Basic authentication of an edge router is done using certificates and RSA cryptography.
- NAT traversal: The Cisco SD-WAN Validator facilitates the initial orchestration between edge routers and Cisco SD-WAN Controllers when one or both of them are behind NAT devices. Standard peer-to-peer techniques are used to facilitate this orchestration.
- Load balancing: In a domain with multiple Cisco SD-WAN Controllers, the Cisco SD-WAN Validator automatically performs load balancing of edge routers across the Cisco SD-WAN Controllers when routers come online.

Cisco SD-WAN Validator is a software module that authenticates the Cisco SD-WAN Controllers and the edge routers in the overlay network and coordinates connectivity between them. It must have a public IP address so that all Cisco vEdge devices in the network can connect to it. (It is the only Cisco vEdge device that must have a public address.)

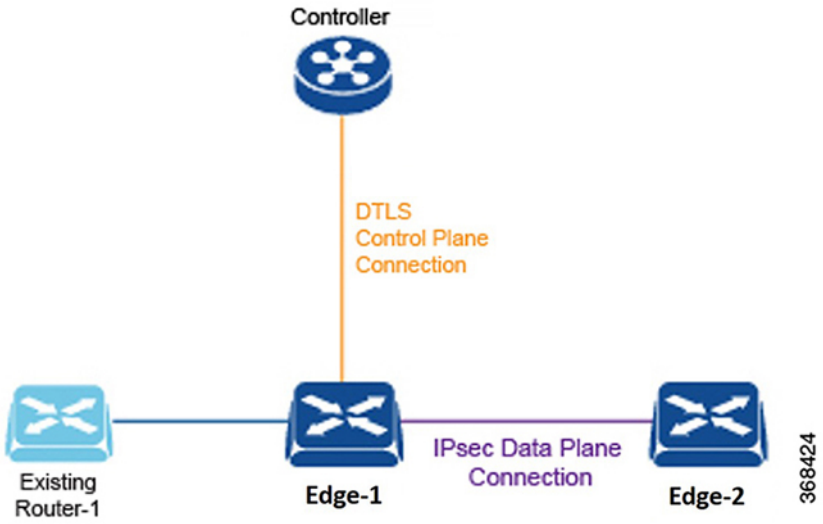
Cisco SD-WAN Validator orchestrates the initial control connection between Cisco SD-WAN Controllers and edge routers. It creates DTLS tunnels to the Cisco SD-WAN Controllers and edge routers to authenticate each node that is requesting control plane connectivity. This authentication behavior assures that only valid customer nodes can participate in the Cisco Catalyst SD-WAN overlay network. The DTLS connections with Cisco SD-WAN Controllers are permanent so that the Cisco SD-WAN Validator controller can inform the Cisco SD-WAN Controllers as edge routers join the network. The DTLS connections with edge routers are temporary; once the Cisco SD-WAN Validator has matched a edge router with a Cisco Catalyst SD-WAN Controller, there is no need for the Cisco SD-WAN Validator and the edge router to communicate with each other. The Cisco SD-WAN Validator shares only the information that is required for control plane connectivity, and it instructs the proper edge routers and Cisco SD-WAN Controllers to initiate secure connectivity with each other. The Cisco SD-WAN Validator maintains no state.

To provide redundancy for the Cisco SD-WAN Validator, you can create multiple Cisco SD-WAN Validator entities in the network and point all edge routers to those Cisco SD-WAN Validators. Each Cisco SD-WAN Validator maintains a permanent DTLS connection with each Cisco Catalyst SD-WAN Controller in the network. If one Cisco SD-WAN Validator becomes unavailable, the others are automatically and immediately able to sustain the functioning of the overlay network. In a domain with multiple Cisco SD-WAN Controllers, the Cisco SD-WAN Validator pairs a edge router with one of the Cisco SD-WAN Controllers to provide load balancing.

Cisco vEdge Devices and Cisco IOS XE Catalyst SD-WAN Devices

The edge router, whether a hardware or software device, is responsible for the data traffic sent across the network. When you place an edge router into an existing network, it appears as a standard router.

Figure 7: An Edge Router Placed into an Existing Network



To illustrate this, the figure here shows an edge router and an existing router that are connected by a standard Ethernet interface. These two routers appear to each other to be Layer 3 end points, and if routing is needed between the two devices, OSPF or BGP can be enabled over the interface. Standard router functions, such as VLAN tagging, QoS, ACLs, and route policies, are also available on this interface.

The components of an edge router are:

- DTLS control plane connection: Each edge router has one permanent DTLS connection to each Cisco SD-WAN Controller it talks to. This permanent connection is established after device authentication succeeds, and it carries encrypted payload between the edge router and the Cisco SD-WAN Controller. This payload consists of route information necessary for the Cisco SD-WAN Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the edge routers.
- OMP (Overlay Management Protocol): As described for the Cisco SD-WAN Controller, OMP runs inside the DTLS connection and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the edge router and the Cisco SD-WAN Controller and carries only control information.
- Protocols: The edge router supports standard protocols, including OSPF, BGP, VRRP, and BFD.
- Routing Information Base (RIB): Each edge router has multiple route tables that are populated automatically with direct interface routes, static routes, and dynamic routes learned via BGP and OSPF. Route policies can affect which routes are stored in the RIB.
- Forwarding Information Base (FIB): This is a distilled version of the RIB that the CPU on the edge router uses to forward packets.
- Netconf and CLI: Netconf is a standards-based protocol used by Cisco SD-WAN Manager to provision a edge router. In addition, each edge router provides local CLI access and AAA.
- Key management: Edge routers generate symmetric keys that are used for secure communication with other edge routers, using the standard IPsec protocol.

- Data plane: The edge router provides a rich set of data plane functions, including IP forwarding, IPsec, BFD, QoS, ACLs, mirroring, and policy-based forwarding.

The edge router has local intelligence to make site-local decisions regarding routing, high availability (HA), interfaces, ARP management, ACLs, and so forth. The OMP session with the Cisco SD-WAN Controller influences the RIB in the edge router, providing non-site-local routes and the reachability information necessary to build the overlay network.

The hardware edge router includes a Trusted Board ID chip, which is a secure cryptoprocessor that contains the private key and public key for the router, along with a signed certificate. All this information is used for device authentication. When you initially start up a edge router, you enter minimal configuration information, such as the IP addresses of the edge router and the Cisco SD-WAN Validator. With this information and the information on the Trusted Board ID chip, the edge router authenticates itself on the network, establishes a DTLS connection with the Cisco SD-WAN Controller in its domain, and receives and activates its full configuration from Cisco SD-WAN Manager if one is present in the domain. Otherwise, you can manually download a configuration file or create a configuration directly on the edge router through a console connection.

Cisco Catalyst SD-WAN Control Connections

The following sections provide information about Cisco Catalyst SD-WAN control connections.

Information About Cisco Catalyst SD-WAN Control Connections

Cisco Catalyst SD-WAN control connections refer to the communication channels that control and manage the operation of a Cisco Catalyst SD-WAN network. These connections are established between Cisco Catalyst SD-WAN control components (Cisco Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Manager) and Cisco IOS XE Catalyst SD-WAN devices.

Support for the TLS 1.3 Protocol

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, the control connections in Cisco Catalyst SD-WAN support the Transport Layer Security protocol version 1.3. The TLS 1.3 version provides stronger security than TLS 1.2, thus improving network performance and efficiency.

If the Cisco Catalyst SD-WAN Control components are using Cisco Catalyst SD-WAN Control Components Release 20.13.1 or later, and devices are using Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, they establish a TLS 1.3 connection between them. In the absence of a TLS 1.3 connection, these components negotiate and establish a connection using TLS 1.2.

Cipher Suites

For control connections, Cisco Catalyst SD-WAN automatically selects one of the following cipher suites:

- TLS-AES-256-GCM-SHA384
- TLS-AES-128-GCM-SHA256
- TLS-AES-128-CCM-8-SHA256
- TLS-AES-128-CCM-SHA256

Benefits of TLS 1.3 in Cisco Catalyst SD-WAN Control Connections

- TLS 1.3 provides stronger security compared to TLS 1.2.
- TLS 1.3 reduces the number of round trips that are required for the initial connection setup (handshake). This reduces latency, and speeds up the establishment of a secure connection, improving overall performance.

Verify Cisco Catalyst SD-WAN Control Connections

The following is a sample output from the **show sdwan control connections** command that displays the connection status, including the TLS version and selected cipher suite. This command displays the information about active control connections and control plane connections on Cisco IOS XE Catalyst SD-WAN devices.

In the following command output, the protocol version (TLS 1.3) and cipher suite are shown in bold.

```
Device# show sdwan control connections

LOCAL-COLOR- lte SYSTEM-IP- 12.16.255.19 PEER-PERSONALITY- vsmart


site-id 100
domain-id 1 protocol tls
protocol-version TLS1_3
cipher-name TLS_AES_256_GCM_SHA384 private-ip 10.0.5.19
private-port 23556
public-ip 10.0.5.19
public-port 23556
org-name vIPtela Inc Regression
state up [Local Err: NO_ERROR] [Remote Err: NO_ERROR] uptime 0:00:01:24
hello interval 1000
hello tolerance 12000
controller-grp-id 0 shared-region-id-set N/A peer-session-id 0xdba4a2f8
Tx Statistics- hello 86
connects 0
registers 0
register-replies 0
challenge 0
challenge-response 1
challenge-ack 0
teardown 0
teardown-all 0
vmanage-to-peer 0
register-to-vmanage 0 Rx Statistics-
hello 86
connects 0
registers 0
register-replies 0
challenge 1
challenge-response 0

challenge-ack 1
teardown 0
vmanage-to-peer 0
register-to-vmanage 0
```

This command displays information about control plane connection attempts initiated by the local device on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan control connection-history detail
```

```
LOCAL-COLOR- lte SYSTEM-IP- 0.0.0.0 PEER-PERSONALITY- vbond


site-id 0
domain-id 0 protocol dtls
protocol-version DTLS1_2
cipher-name ECDHE-RSA-AES256-GCM-SHA384
private-ip 10.0.12.26
private-port 12346
public-ip 10.0.12.26
public-port 12346
UUID/chassis-number eb8844be-f58f-4bd3-b8c2-4f8cbc78131c
state tear_down [Local Err: ERR_DISCONNECT_VBOND] [Remote Err: NO_ERROR] downtime
2023-10-13T20:06:44+0000
repeat count 0 previous downtime N/A
Tx Statistics- hello 17
connects 0
registers 2
register-replies 0
challenge 0
challenge-response 1
challenge-ack 0
teardown 1
teardown-all 0
vmanage-to-peer 0
register-to-vmanage 0 Rx Statistics-

hello 17
connects 0
registers 0
register-replies 2
challenge 1
challenge-response 0
challenge-ack 1
teardown 0
vmanage-to-peer 0
register-to-vmanage 0
```

This command displays information about control plane connection attempts initiated by a Cisco IOS XE Catalyst SD-WAN device toward Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller.

```
Device# show control connections detail""
-------------------------------------------------------------------------------------------------

 REMOTE-COLOR- lte SYSTEM-IP- 172.16.255.21   PEER-PERSONALITY- vedge
-------------------------------------------------------------------------------------------------
site-id             100
domain-id           1
protocol            tls
protocol-version    TLS1_2
cipher-name         ECDHE-RSA-AES256-GCM-SHA384
private-ip          10.0.111.1
private-port        46437
public-ip           10.0.111.1
public-port         46437
org-name            vIPtela Inc Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:10:02
hello interval      1000
hello tolerance     12000
peer-session-id      0x00656994de

  Tx Statistics-
  --------------
    hello                   603
```

```
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    teardown-all            0
    vmanage-to-peer         1
    register-to-vmanage     0
    create-cert-reply       0

  Rx Statistics-
  --------------
    hello                   603
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     1
    create-cert             0

-------------------------------------------------------------------------------------------------

 REMOTE-COLOR- default SYSTEM-IP- 172.16.255.19   PEER-PERSONALITY- vsmart
-------------------------------------------------------------------------------------------------
site-id             100
domain-id           1
protocol            tls
protocol-version    TLS1_3
cipher-name         TLS_AES_256_GCM_SHA384
private-ip          10.0.5.19
private-port        23456
public-ip           10.0.5.19
public-port         23456
org-name            vIPtela Inc Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:09:48
hello interval      1000
hello tolerance     12000
peer-session-id      0x00b6655c4d

  Tx Statistics-
  --------------
    hello                   589
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                0
    teardown-all            0
    vmanage-to-peer         1
    register-to-vmanage     0
    create-cert-reply       0

  Rx Statistics-
  --------------
    hello                   589
```

```
connects                0
registers               0
register-replies        0
challenge               1
challenge-response      0
challenge-ack           1
teardown                0
vmanage-to-peer         0
register-to-vmanage     1
create-cert             0
```

Cisco Catalyst SD-WAN Solution

To streamline and optimize cloud networking, Cisco Catalyst SD-WAN offers next-generation software services that run on the secure, virtual IP fabric:

- **Cloud onRamp for SaaS**: Cloud onRamp for SaaS optimizes the performance of Software as a Service (SaaS) cloud applications. It provides clear visibility of the performance of individual applications and automatically chooses the best path for each one. Cloud onRamp calculates metrics about loss and latency using a formula customized for each application.
- **Cisco SD-WAN Analytics**: Cisco SD-WAN Analytics is a SaaS service hosted by Cisco Catalyst SD-WAN as part of the solution. It provides graphical representations of the performance of your entire overlay network over time and lets you drill down to the characteristics of a single carrier, tunnel, or application at a particular time.
- **Cisco Catalyst SD-WAN Portal**: Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool tailored for Cisco Catalyst SD-WAN, which provides a quick way to provision, monitor, and maintain Cisco SD-WAN Controllers on public cloud providers.

Cloud onRamp for SaaS

Enterprises have been adopting business critical SaaS applications including Microsoft Office365, Salesforce, Dropbox, and others. Enterprises use three primary methods to offer connectivity to SaaS applications for their users:

• Direct Internet Access (DIA) from a branch office.

• Internet access through gateways in regional facilities.

• Cloud exchange or direct connection through gateways in a Carrier Neutral Facility (CNF).

Latency and packet loss have a direct impact on the performance of applications and on end-user experience, but in many cases network administrators have limited or no visibility into the network performance characteristics between the end-user and SaaS applications. When path impairment occurs and application performance suffers, shifting traffic from a primary to an alternate path usually requires the network administrator to performa a set of complex, manual, time-consuming, and error-prone steps.

Cisco Catalyst SD-WAN Cloud onRamp for SaaS provides visibility and continuous monitoring of network performance characteristics. It makes real-time decisions by choosing the best performing path between the end-user and SaaS application for an optimal user experience. It automatically reacts to changes in network performance by intelligently re-routing application traffic away from any degraded network paths.

Cloud onRamp for SaaS supports all access methods for cloud-based SaaS applications, including DIA, internet access through a regional facility, and access through a CNF.

Cloud onRamp for SaaS calculates an application performance value called the Viptela Quality of Experience (vQoE) for enterprise cloud applications. The vQoE value weighs loss and latency using a formula customized for each application. For example, email applications tolerate latency better than video applications do, and video applications tolerate loss better than email does. The vQoE value ranges from zero to ten, with zero being the worst quality and ten being the best.

You enable Cloud onRamp for SaaS in Cisco SD-WAN Manager with a few clicks of the mouse, and then you access the Cloud onRamp dashboard in Cisco SD-WAN Manager for continuous visibility into the performance of individual applications.

Cisco Catalyst SD-WAN Analytics

Cisco SD-WAN Analytics offers visibility into the performance of applications and the network over time. Cisco SD-WAN Analytics is a SaaS service hosted by Cisco Catalyst SD-WAN as part of the solution. It provides graphical representations of your entire overlay network and lets you drill down to display the characteristics of a single carrier, tunnel, or application at a particular time.

The Cisco SD-WAN Analytics dashboard serves as an interactive overview of your network and an entrance point for more details. The dashboard by default displays information aggregated for the last 24 hours. When you drill down, you can select different time periods for different data sets to display. The dashboard displays data on application performance, WAN site usage, and carrier usage.

Cisco SD-WAN Analytics calculates application performance with the QoE value, which is customized for individual applications. This value ranges from zero to ten, with zero being the worst performance and ten being the best. Cisco SD-WAN Analytics calculates QoE based on latency, loss, and jitter, customizing the calculation for each application.

Cisco SD-WAN Analytics stores data over a long period of time, displays historical trend information, and offers insights that could be used for future planning.

It offers:

- Application visibility:
  - Best and worst performing applications: Display the best and worst performing applications and drill down to details at the site level.
  - Most bandwidth consuming applications: Display applications consuming the most bandwidth and drill down to sites and users.
- Network visiblity:
  - Network availability and circuit availability: Display network availability and correlate network and circuit availability.
  - Tunnel performance: Display key performance indicators such as loss, latency and jitter over various Cisco Catalyst SD-WAN tunnels.
  - Carrier usage views: Display providers and their network characteristics.

Cisco Catalyst SD-WAN Portal

Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool tailored for Cisco Catalyst SD-WAN, which provides a quick way to provision, monitor, and maintain Cisco SD-WAN Controllers on public cloud providers.

You can provision the following controllers using the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN Controller

Note Beginning with Cisco vManage Release 20.9.1, a link to the Cisco Catalyst SD-WAN Portal is added from the Cisco Catalyst SD-WAN menu. From the Cisco Catalyst SD-WAN menu, click **SD-WAN Portal** to access the Cisco Catalyst SD-WAN Portal for provisioning, monitoring, and maintaining Cisco SD-WAN Controllers.

For more information on the Cisco Catalyst SD-WAN Portal, see the *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Cisco SD-AVC

Beginning with the 18.4 release, Cisco Catalyst SD-WAN incorporates Cisco Software-Defined Application Visibility and Control (SD-AVC) to provide:

- Recognition of network application traffic for visibility, analytics, application-aware routing, and application-based policies, such as QoS and application-based firewall policy.
- Analytics at the network level.

Cisco SD-AVC operates on Cisco IOS XE Catalyst SD-WAN devices in the network, and the Cisco SD-AVC network service operates as a container within Cisco SD-WAN Manager.

Note All relevant Cisco SD-AVC functionality is accessed through the Cisco SD-WAN Manager interface. Cisco Catalyst SD-WAN does not support the use of a separate SD-AVC interface.

Cisco SD-WAN Manager Cluster

Cisco SD-AVC must operate on only one Cisco SD-WAN Manager instance. In a Cisco SD-WAN Manager cluster, enable Cisco SD-AVC on only one instance of Cisco SD-WAN Manager.

Work with Cisco Catalyst SD-WAN

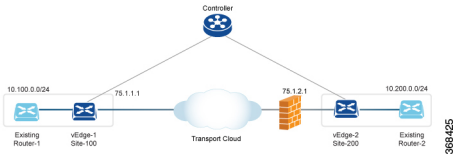
Build a Basic Overlay Network using Cisco vEdge Devices

Let's use a simple network design, one that has two vEdge routers and one Cisco SD-WAN Controllers, to illustrate how to form a functioning overlay network from Cisco vEdge components. In this topology, the Cisco SD-WAN Validator software has been enabled on one of the vEdge routers. Once you understand a simple network, you can start designing and building more complex topologies.

A Simple Network Topology

The following figure illustrates our simple topology. Here, we have two sites, Site-100 and Site-200. vEdge-1 is the edge device in Site-100, and vEdge-2 is the edge device at Site-200. At each local site, the vEdge router connects to an existing traditional router via a standard Ethernet interface. vEdge-2 is connected to the transport network through a NAT device that also has firewall functionality.

Figure 8: A Simple Network Topology



The goal of our design is to create a private network so that Router-1 and Router-2 can be next to each other from a Layer 3 perspective and so that hosts connected to each of these routers can communicate through the private network.

Construct a Basic Network

The following steps allow you to create the simple overlay network depicted in the topology above.

- Step 1: Perform initial bringup and basic configuration.
- Step 2: Enable host or service-side interfaces and routing.
- Step 3: Enable overlay routing over OMP.
- Step 4: Check the automatic setup of the IPsec data plane.
- Step 5: Enforce policies.

Let's look at the steps in a bit more detail.

Step 1: Perform Initial Bring up and Basic Configuration

From the perspective of a network administrator, the initial bringup of the Cisco vEdge network components is a straightforward and simple process, involving creating the configurations for each of the network components and ensuring that a few key authentication-related files are in place. From the perspective of user, bringup entails simply powering up the vEdge router and plugging in a cable to connect the router to the network. The remainder of the bringup occurs automatically via a zero-touch-provisioning process.

The network administrator performs the following tasks as part of the initial bringup:

1. Configure the Cisco SD-WAN Validator function on one of the vEdge routers in the network. In our example, this is vEdge-1.
2. Optionally, configure a top-level Cisco SD-WAN Validator to act as a ZTP server. In this situation, a DNS server must be present in the enterprise network.
3. Ensure that a DHCP server is present in the enterprise network.
4. Install the signed certificate on Cisco SD-WAN Manager, and download that certificate to Cisco SD-WAN Manager orchestrator.
5. Install the vEdge router authorized serial number file on Cisco SD-WAN Manager, and then download it to the Cisco SD-WAN Controllers.

6. From Cisco SD-WAN Manager CLI, create a configuration for each Cisco Catalyst SD-WAN Controller and vEdge router in the overlay network:

   a. Configure a system IP address, which is similar to the router ID address on a traditional router, identifying the Cisco vEdge device with an address that is independent of any of the interfaces on the device. System IP addresses must be pre-allocated and must be unique across each vEdge router and Cisco Catalyst SD-WAN Controller. These addresses need not be routable through the network.

   b. Configure site IDs for the various sites in the overlay network. In our example, vEdge-1 is at site-100 and vEdge-2 is at site-200. The Cisco Catalyst SD-WAN Controller can be collocated at a site, or it can be in its own site.

   c. Configure domain IDs. This is an optional step to create clusters. For our example, configure the domain-ID as 1.

   d. Configure the IP address or DNS name for the Cisco SD-WAN Validator server and the Cisco Catalyst SD-WAN Controller.

   e. Configure WAN interfaces on vEdge-1 and vEdge-2. VPN 0 is the VPN reserved for WAN transport interfaces. IP addresses can be automatically obtained through DHCP. Alternatively, you can configure a default gateway and DNS explicitly.

   f. By default, DTLS and IPsec are enabled on the WAN interfaces.

   g. Save the configuration.

When the Cisco SD-WAN Controllers join the network, they are authenticated by the Cisco SD-WAN Validator, and when vEdge routers join the network, they are authenticated by both the Cisco SD-WAN Validator and the Cisco SD-WAN Controllers. These devices then connect to Cisco SD-WAN Manager, which downloads the configuration to them.

Example Configuration on vEdge-1:

```
system
  host-name vEdge-1
  system-ip 1.0.0.1
  domain-id 1
  site-id   100
  vbond 75.1.1.1  local
!
vpn 0
  interface ge 0/0
    ip address 75.1.1.1/24
    tunnel-interface
      color default
    no shutdown
  ip route 0.0.0.0/0 75.1.1.254
!
```

The remaining sections in this article describe how to configure other common functionality on vEdge routers and Cisco SD-WAN Controllers. Typically, you configure all functionality at one time, in the configuration that you create on Cisco SD-WAN Manager and that is downloaded to the device when it joins the overlay network. However, to highlight the different functionalities, this article describes the various portions of the configuration separately.

Step 2: Enable Host or Service-Side Interfaces and Routing

From Cisco SD-WAN Manager, you can also configure service-side interfaces and regular routing:

1. Configure interfaces on vEdge-1 towards the existing traditional router. Assign IP address and put the interface in a non-default VPN. In our example, this is VPN 1. Do the same on vEdge-2.
2. Configure OSPF or BGP on the vEdge routers towards the existing routers
3. Commit

To check for standard IP reachability, routes, and next hops at the local site, use the standard **ping**, **traceroute**, and various **show** commands on Cisco SD-WAN Manager or from the CLI of the device (if you have a direct connection to the device):

Example Configuration for the Host or Service-side VPN:

```
vpn 1
  router
    ospf
      redistribute omp
      area 0
        interface ge 0/1
        exit
      exit
    !
  !
  interface ge 0/1
    ip address 10.1.2.12/24
    no shutdown
!
```

Step 3: Enable Overlay Routing over OMP

All site-local routes are populated on the vEdge routers. Distributed these routes to the other vEdge routers this is done through the Cisco Catalyst SD-WAN Controller, via OMP.

1. If you are using BGP or if there are OSPF external LSAs, allow OMP to redistribute the BGP routes.
2. Re-advertise OMP routes into BGP or OSPF.
3. Commit.

Example Configuration of Overlay Routing over OMP:

```
omp
  advertise ospf external
!
```

At this point, vEdge-1 is able to learn about the prefixes from site-200, and vEdge-2 is able to learn about prefixes from site-100. Because all the prefixes are part of VPN 1, the hosts in site-100 and site-200 have reachability with one another. From a Cisco Catalyst SD-WAN overlay network point of view, this reachability is possible because vEdge-1 advertises a vRoute consisting of the address 10.100.0.0/24 and the TLOC color of default, which we write as {75.1.1.1, default }, to the Cisco Catalyst SD-WAN Controller. In turn, the Cisco Catalyst SD-WAN Controller advertises this vRoute to vEdge-2. The same process happens with prefix 10.200.0.0/24 on vEdge-2.

Step 4: Check the Automatic Setup of the IPsec Data Plane

For every TLOC on a vEdge router, the vEdge router advertises a symmetric key for encryption. The Cisco Catalyst SD-WAN Controller reflects this key automatically and advertises the TLOC with the symmetric key. A two-way IPsec SA is set up as a result (that is, there is a different key in each direction), and data traffic

automatically starts to use this IPsec tunnel. Once a tunnel is up, BFD automatically starts on the tunnel. This is done to ensure fast data plane convergence in the event of a failure in the transport network.

The setup of the IPsec data plane happens automatically. No configuration is necessary. Multiple show commands are available to check the SAs and the state of the IPsec tunnel.

Step 5: Enforce Policies

As an optional step, you can create control and data plane policies on the Cisco Catalyst SD-WAN Controller and push them to the vEdge routers. As an example, if the network administrator wants to enforce a policy to divert traffic destined to { vEdge-2, prefix 10.200.0.0/24 } to go to another site say vEdge-3, a control plane policy can be created on the Cisco Catalyst SD-WAN Controller and pushed to the respective vEdge routers. The results of the policy are pushed to the vEdge routers, not the configuration itself.

Example Configuration of Policies:

```
policy
  lists
    site-list site-100
      site-id 100
    !
    prefix-list my-prefixes
      ip-prefix 10.200.0.0/24
    !
  control-policy TE-thru-vedge3
    sequence 10
      match route
        prefix-list my-prefixes
      !
      action accept
        set
          tloc 1.0.0.3 color default
        !
      !
      default action accept
    !
apply-policy
  site-list site-100
    control-policy TE-thru-vedge3 out
  !
!
```

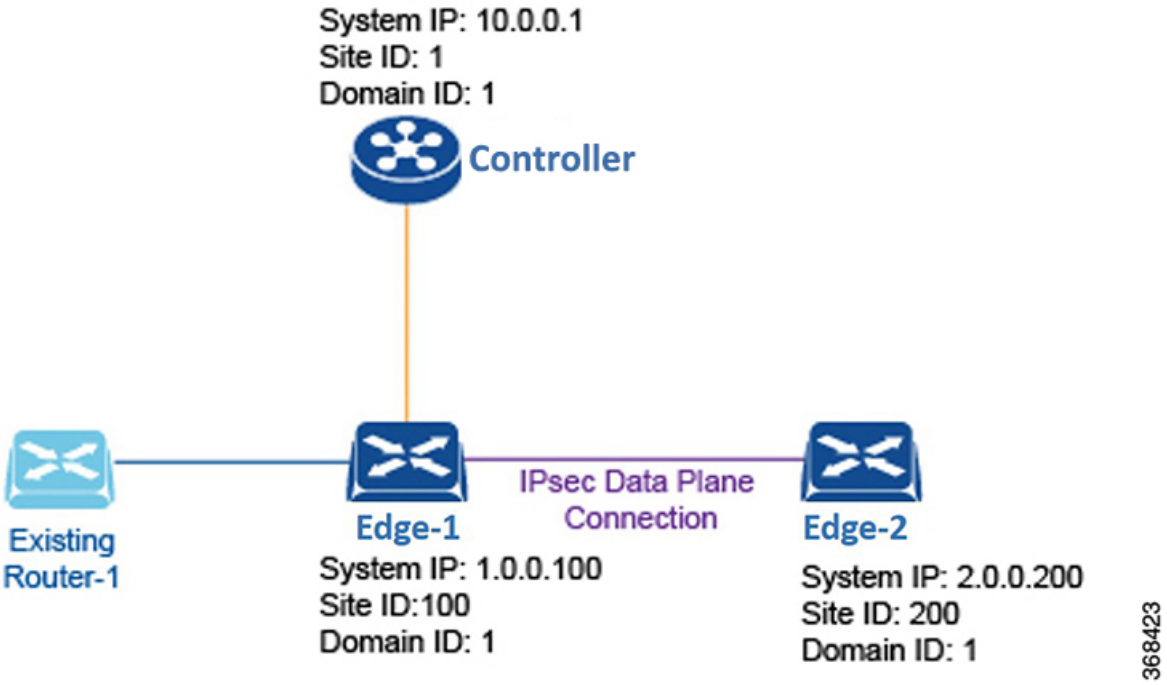
Advanced Options

Now that we have looked at basic routing, security, and policy, we can start adding various other elements to the network. You are encouraged to look at the *Software* category to add elements such as High Availability, Convergence, BFD, QoS, ACLs, segmentation, and advanced policy.

Cisco Catalyst SD-WAN Terminology

The following figure summarizes the terminology used to describe a Cisco Catalyst SD-WAN overlay network.

Figure 9: Terminology used in a Cisco Catalyst SD-WAN overlay network



Domain ID

A domain is a logical grouping of edge routers and Cisco SD-WAN Controllers that demarcate the span of control for the Cisco SD-WAN Controllers. Each domain is identified by a unique integer, called the domain ID. Currently, you can configure only one domain in a Cisco Catalyst SD-WAN overlay network.

Within a domain, edge routers can connect only with the Cisco SD-WAN Controllers in their own domain. The Cisco SD-WAN Validator is aware of which Cisco SD-WAN Controllers are in which domain, so that when new edge routers come up, the Cisco SD-WAN Validator can point those routers to the Cisco SD-WAN Controllers in the proper domain. However, the Cisco SD-WAN Validator is never a member of a domain.

Within a domain, there is full synchronization of routing information among the Cisco SD-WAN Controllers and edge routers, and there is scope for route aggregation and summarization. An organization can divide up its network into domains to serve desired business purposes. For example, domains can correspond to a large geographic area or to data centers so that each data center and the branches for which it is responsible are contained within a single domain.

OMP Routes

On Cisco SD-WAN Controllers and edge routers, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called Transport Locations (TLOCs). These routes are called OMP routes, to distinguish them from standard IP routes. It is through OMP routes that the Cisco SD-WAN Controllers learn the network topology and the available services.

Cisco Catalyst SD-WAN control plane architecture uses three types of OMP routes:

- OMP routes: Prefixes that establish reachability between end points that use the OMP-orchestrated transport network. OMP routes can represent services in a central data center, services at a branch office, or collections of hosts and other end points in any location of the overlay network. OMP routes require and resolve into TLOCs for functional forwarding. In comparison with BGP, an OMP route is the equivalent of a prefix carried in any of the BGP AFI/SAFI fields.
- TLOCs: Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it must be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.
- Service routes: Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, Intrusion Detection Systems (IDPs), and load balancers.



Note The maximum OMP routes supported are 140K on the C1131X_8PW devices. When there are more than 140K OMP routes, the device crashes due to the out of memory issue.

Site ID

A site is a particular physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each Cisco vEdge device at a site is identified by the same site ID. So within a data center, all the Cisco SD-WAN Controllers and any edge routers are configured with the same site ID. A branch office or local site typically has a single edge router, but if a second one is present for redundancy, both routers are configured with the same site ID.

System IP Address

Each edge router and Cisco Catalyst SD-WAN Controller is assigned a system IP address, which identifies the physical system independently of any interface addresses. This address is similar to the router ID on a regular router. The system IP address provides permanent network overlay addresses for edge routers and Cisco SD-WAN Controllers, and allows the physical interfaces to be renumbered as needed without affecting the reachability of the Cisco vEdge device. You write the system IP address as you would an IPv4 address, in decimal four-part dotted notation.

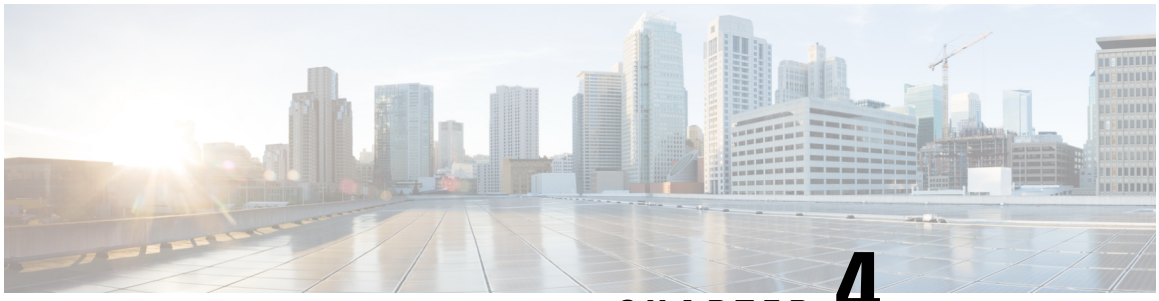
TLOC

A TLOC, or transport location, identifies the physical interface where a edge router connects to the WAN transport network or to a NAT gateway. A TLOC is identified by a number of properties, the primary of which is an IP address–color pair, which can be written as the tuple {IP-address, color}. In this tuple, IP address is the system IP address and color is a fixed text string that identifies a VPN or traffic flow within a VPN. OMP advertised TLOCs using TLOC routes.

Additional Information

For a description of the elements in a Cisco Catalyst SD-WAN overlay network, see *Components of the Cisco Catalyst SD-WAN Solution*. For an understanding of how you put together an overlay network using Cisco

Catalyst SD-WAN software and hardware, see *Constructing a Basic Network Using Cisco Catalyst SD-WAN Components*. For examples of how the components of the overlay network work, see the *Validated Examples*.



CHAPTER 4

Hardware and Software Installation

Table 2: Feature History

Feature Name	Release Information	Description
Generate a Bootstrap File For Cisco IOS XE Catalyst SD-WAN Devices Using the CLI	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This feature enables you to generate a minimum bootstrap configuration file directly on a device, that enables a device to reconnect to the controller in case the full configuration is ever lost or removed.

- Server Recommendations, on page 33
- Device Configuration Reset of Cisco IOS XE Catalyst SD-WAN devices after Adding or Removing Modules, on page 34
- On-Site Bootstrap Process for Cisco Catalyst SD-WAN Devices, on page 34
- On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates, on page 37
- Generate a Bootstrap File For Cisco IOS XE Catalyst SD-WAN Devices Using the CLI, on page 42
- One Touch Provisioning: Onboard Cisco IOS XE Catalyst SD-WAN Devices Using Generic Bootstrap Configuration, on page 44
- Software Installation and Upgrade for Cisco IOS XE Routers, on page 48
- Recover the Default Password, on page 57
- Software Installation and Upgrade for vEdge Routers, on page 58
- Upgrade Memory and vCPU Resources on a Virtual Machine Hosting Cisco Catalyst SD-WAN Manager, on page 66
- Expand the secondary disk size, Cisco Catalyst SD-WAN Manager Release 20.12.x and later, on page 68
- Software Maintenance Upgrade for Cisco IOS XE Catalyst SD-WAN Devices, on page 69

Server Recommendations

This topic links to the hardware recommendations for the Cisco SD-WAN Validator server, vEdge Cloud router server, Cisco SD-WAN Manager server, and Cisco SD-WAN Controller server: Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

vEdge Cloud Router Server Recommendations

Refer to vEdge Cloud Datasheet.

Device Configuration Reset of Cisco IOS XE Catalyst SD-WAN devices after Adding or Removing Modules

Prerequisites

You should have a basic knowledge of router modules hardware installation. For information on how to insert or remove modules from a platform, see the respective platform or module documentation.

OIR Support



Note OIR is not supported on Cisco IOS XE Catalyst SD-WAN devices.

Online Insertion and Removal (OIR) enables you to replace parts in a Cisco device without affecting the system operation. When a module is inserted, power is available on the module, and it initializes itself to start working.

Hot swap functionality allows the system to determine when a change occurs in the unit's physical configuration, and reallocate the unit's resources to allow all interfaces to function adequately. This feature allows interfaces on the module to be reconfigured while other interfaces on the router remain unchanged.

The software performs the necessary tasks involved in handling the removal and insertion of the module. A hardware interrupt is sent to the software subsystem when a hardware change is detected, and the software reconfigures the system as follows:

- When a module is inserted, it is analyzed and initialized in such a way that the end user can configure it properly. The initialization routines used during OIR are the same as those called when the router is powered on. System resources, also handled by software, are allocated to the new interface.
- When a module is removed, the resources associated with the empty slot must either be freed or altered to indicate the change in its status.

Reset Device Configuration

When a module is inserted or removed from your Cisco IOS XE Catalyst SD-WAN devices, you must perform a device configuration reset using the CLI to keep Cisco IOS XE Catalyst SD-WAN device synchronized with the physical change. For more information about resetting the controller mode configuration, see Controller Mode Configuration Reset.

On-Site Bootstrap Process for Cisco Catalyst SD-WAN Devices

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive or from internal boot flash to a device that supports Cisco Catalyst SD-WAN. When the device boots, it uses the information in the configuration file to come up on the network.

The on-site bootstrap process consists of this general workflow:

- Use Cisco SD-WAN Manager to generate a configuration file
- Copy the configuration file to a bootable USB drive and plug the drive into a device, or copy the configuration to the bootflash of a device
- Boot the device

If the configuration file is on both an inserted USB drive and on the bootflash, a device gives priority to the configuration file on the bootflash.

Device Requirements

A device that you configure by using the on-site bootstrap process must meet these requirements:

- A supported Cisco Catalyst SD-WAN image is installed on the device.
- The device is in its factory state with no added configuration.

Restrictions

- Onboarding using a bootstrap file does not support configuring cellular interfaces or other NIM module-specific configurations. If you need to configure these, push a full configuration after onboarding.
- When features that require Cisco SD-WAN Manager side encryption are included in bootstrap, it can cause bootstrap and PNP failure. Cisco SD-WAN Manager and device cannot share the same secret keys. You cannot use Cisco SD-WAN Manager encrypted configuration in bootstrap directly on the device.
- Do not include policy configuration in the bootstrap file. If you need to configure policy, do this as part of a full configuration after onboarding.

Perform the On-Site Bootstrap Process

To perform the on-site bootstrap process for a device, follow these steps:

1. Upload the Chassis ID and the serial number of the device to Cisco SD-WAN Manager.

   For instructions, see *Upload the vEdge Serial Number File*.

2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and make sure that the Organization Name and the Cisco Catalyst SD-WAN Validator IP address are configured properly.

3. If you are using your own enterprise root certificate authority (CA) for device certification in your network, take these actions in Cisco SD-WAN Manager:

   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

   b. Click **WAN Edge Cloud Certificate Authorization**.

      (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.)

   c. Click **Manual**.

   d. Click **Save**.

4. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

5. Click **Feature Templates** and create a template for the device.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

6. Perform the following steps:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. For the desired device, click **...** and choose **Generate Bootstrap Configuration**.
   c. In the dialog box, choose **Cloud-init** and click **OK**.

      The system generates a Multipurpose Internet Mail Extensions (MIME) file and displays its contents in a pop-up window. This file contains system properties for the device, the root CA if you are using an enterprise root CA, and configuration settings from the template that you created.
7. In the MIME file pop-up window, click **Download**.

   The system downloads the file to your local system and saves it in your directory for downloads. The file name is chassis.cfg, where chassis is the device chassis ID that you uploaded in Step 1.

Note As an alternative to this step, you can copy the contents of the MIME file from the pop-up window to a text file, save the text file with the name `ciscosdwan.cfg` (case sensitive), and then skip to Step 8.

Note For hardware devices, use the bootstrap file name as `ciscosdwan.cfg`. This file is generated by Cisco SD-WAN Manager and includes UUID, but does not include OTP. For software devices (CSR and ISRv), and OTP-authenticated devices such as ASR1002-X, use the bootstrap file name as `ciscosdwan_cloud_init.cfg`. This file contains the OTP but not the UUID validation for `ciscosdwan_cloud_init.cfg`.

8. If you downloaded the MIME file, rename it to `ciscosdwan.cfg` (case sensitive).

Note This is the configuration file for the on-site bootstrap process.

9. Copy the `ciscosdwan.cfg` file to a bootable USB drive or to the bootflash of the device.

Note The file must be named exactly as shown or the device will not read it.

10. If you are using a USB drive, plug the USB drive into the device.
11. Boot the device.

The device reads the configuration file from the USB drive or the bootflash and uses the configuration information to come up on the network. The device give priority to a configuration file that is on its bootflash.

On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates

Table 3: Feature History

Feature Name	Release Information	Description
On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	By default, a Cisco vEdge 5000 device uses an SHA1 certificate for authentication with controllers in the overlay network. With this feature, you can authenticate the device using an OTP and a Public Key, and install an SHA2 enterprise certificate on the device. By authenticating the device using an OTP and a Public Key and installing an SHA2 enterprise certificate, you can bypass SHA1 certificate authentication and secure the device against SHA1 vulnerabilities.

A Cisco vEdge 5000 device is equipped with a Trusted Platform Module (TPM 1.2) and uses SHA1 certificates for authentication while connecting to the overlay network. For information on the bootstrap process using SHA1 certificates, see *On-Site Bootstrap Process for Cisco Catalyst SD-WAN Devices.*

From Cisco Catalyst SD-WAN Release 20.3.1, while bootstrapping a Cisco vEdge 5000 device and connecting the device to the overlay network, you can authenticate the device using a One Time Password (OTP) and a Public Key, and install an SHA2 enterprise certificate on the device. By authenticating the device using an OTP and a Public Key and installing an SHA2 enterprise certificate, you can bypass SHA1 certificate authentication and secure the device against SHA1 vulnerabilities.

How Cisco vEdge 5000 is Authenticated using OTP and Public Key

1. Enter the public key for the device on **Plug and Play Connect** and generate the `serial.viptela` file.
2. Upload the `serial.viptela` file to Cisco SD-WAN Manager.
3. Cisco SD-WAN Manager generates a random authentication token for the device. Cisco SD-WAN Manager encrypts the authentication token using the device public key and populates it as the OTP in the `<chassis>.config` file.
4. Download the `<chassis>.config` file to a bootable USB drive and insert the USB drive into the device after performing a factory reset.

5. The device reads the `<chassis>.config` file, reads the encrypted digest from the OTP field, decrypts the digest using the device private key and obtains the authentication token.
6. The device disables AVNET/TPM1.2 SHA1 certificate authentication.
7. The device authenticates itself with Cisco SD-WAN Manager using the authentication token and establishes a control connection.
8. Cisco SD-WAN Manager pushes the initial configuration into the device.
9. Cisco SD-WAN Manager pushes the SHA2 enterprise certificate for the device and installs the certificate on the device.
10. Device reauthenticates itself to controllers using the SHA2 enterprise certificate and connects to controllers.

Points to Consider

- After a Cisco vEdge 5000 device is authenticated with Cisco SD-WAN Validator or Cisco SD-WAN Manager using OTP, do not reboot the device until the SHA2 enterprise certificate is installed and validated. If the device reboots before the Enterprise Certificate is validated, restart the bootstrap procedure.
- After a signed SHA2 enterprise certificate is installed on a Cisco vEdge 5000 device and the bootstrapping process is complete, if you perform a software reset, a configuration reset, or a factory reset, bootstrap the device again.
- Every time you generate the Cloud-Init(Encrypted OTP) bootstrap configuration, you must download the new configuration file to a bootable USB drive.

Prerequisites

1. Ensure Enterprise Certificate authorization is configured.
   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
   b. Click **Hardware WAN Edge Certificate Authorization**.

      (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.)
   c. Ensure that **Enterprise Certificate (signed by Enterprise CA)** is selected and click **Save**.
2. Ensure that the public key entry for the device is available on the PNP server before generating the `serial.viptela` file. For more information, see *View or Add Public Key for a Cisco vEdge 5000 Device*.
3. If a Cisco vEdge 5000 device is connected to the overlay network using SHA1 certificates, you must invalidate and remove the device from the overlay network before configuring the use of OTP, Public Key, and SHA2 enterprise certificate for authentication.

View or Add Public Key for a Cisco vEdge 5000 Device

1. On Cisco Software Central, log in to **Plug and Play Connect** using the required Smart and Virtual Accounts required to access the Cisco vEdge 5000 device.
2. In the **Devices** list, click on the serial number of the Cisco vEdge 5000 device.

The **Device Information** is displayed.

3. In the **Device Information** dialog box, check whether the device **Public Key** is available.
4. If the **Public Key** is not available, add the **Public Key**:
   a. In the **Devices** list, select the Cisco vEdge 5000 device using the check box.
   b. Click **Edit**.

      The **Edit Devices** page is displayed.
   c. In the **Selected Devices** area, click **view/edit** in the **Public Key** column.

      The **Public Key** dialog box is displayed.
   d. Enter the public key in the text box, or click **Browse** to upload a file containing the public key.
   e. Click **OK** to save the public key and close the dialog box.
   f. On the **Edit Devices** page, click **Submit** to attach the public key to the Cisco vEdge 5000 device.

Bootstrap Procedure

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive. When the Cisco vEdge 5000 device boots, it uses the information in the configuration file to connect to the overlay network.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Click **Upload WAN Edge List**.
3. In the **Upload WAN Edge List** dialog box, select the the Cisco vEdge 5000 serial number file to upload. Select **Validate the uploaded vEdge list and send to controllers** and click **Upload**.

   The WAN Edge List is uploaded to controllers.

   The Cisco vEdge 5000 device is added to the **WAN Edge List**.
4. Attach the device to a device configuration template.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device** and select a template.
   c. For the desired template, click **...** and choose **Attach Devices**. The **Attach Devices** dialog box opens.
   d. In the **Available Devices** column, select a group, and search to select the Cisco vEdge 5000 device.
   e. Click the arrow pointing right to move the device to the **Selected Devices** column.
   f. Click **Attach**.

      Configuration template is scheduled for the device.
5. Generate the bootstrap configuration for the newly added device.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. Click **WAN Edge List**, select the Cisco vEdge 5000 device.

c. For the selected device, click **...** and choose **Generate Bootstrap Configuration**.

d. In the **Generate Bootstrap Configuration** dialog box, select **Cloud-Init(Encrypted OTP)** and click **OK**.

e. Click **Download** to download the bootstrap configuration and save the file with a filename in the `<ChassisNumber>.cfg` format.

f. Copy the `<ChassisNumber>.cfg` file to a bootable USB drive.



Note

- The USB drive must be of the FAT-32 format for Cisco vEdge 5000 device to recognize and auto-mount the drive.
- Copy the `<ChassisNumber>.cfg file` to the home or parent directory of the USB drive.

6. Send the Cisco vEdge 5000 serial number file and OTP information to controllers.

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**.

   b. Click **Send to Controllers** to synchronize the WAN Edge list on all controllers.

   The device serial number file and OTP information are sent to controllers.

   c. (Optional) Verify the WAN Edge List on controllers using the command **show orchestrator valid-vedges hardware-installed-serial-number prestaging**.

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number prestaging

 HARDWARE

  INSTALLED   SUBJECT

  SERIAL      SERIAL
CHASSIS NUMBER  SERIAL NUMBER                    VALIDITY  ORG
  NUMBER      NUMBER
-------------------------------------------------------------------------------------------------
193A0122170001  deaedf5d39919454fdfcc8470eccd8d8  valid     vIPtela Inc Regression
  prestaging  N/A
```

7. Perform a factory reset of the Cisco vEdge 5000 device with a default image of Cisco SD-WAN Release 20.3.1 or later.

8. When the Cisco vEdge 5000 device is ‘Up’ (indicated by a status of ‘System: Up’ on the LCD display), insert the USB drive with `<ChassisNumber>.cfg` file.

   The device reads the `<ChassisNumber>.cfg` file from the USB drive. Organization-name, Cisco SD-WAN Validator IP address, OTP token, and Enterprise root-ca are retrieved from the configuration file.

   a. (Optional) Issue the **show control local-properties** command on the device to verify the information retrieved from the configuration file.

   b. (Optional) If the device WAN interface is not assigned an IP address through DHCP, configure a static IP address and the routing information required to reach controllers.

The device connects to Cisco SD-WAN Validator and Cisco SD-WAN Manager after authentication using the OTP.

The device obtains the System IP address and the site ID from Cisco SD-WAN Manager configuration templates. If templates are not configured on Cisco SD-WAN Manager, configure the required system configuration on the device.

After the device connects to Cisco SD-WAN Manager, Cisco SD-WAN Manager retrieves the Enterprise Certificate Signing Request (CSR). From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, the device certificate state is shown as **CSR**.

9. Download CSR.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
   b. Select the Cisco vEdge 5000 device for which to sign a certificate.
   c. For the selected device, click **...** and select **View Enterprise CSR**.
   d. To download the CSR, click **Download**.
10. Send the certificate to a third-party signing authority and have them sign it.
11. To install the certificate on the device, perform the following steps:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **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.

   b. Click **Install Certificate** button located in the upper-right corner of the screen.
   c. In the **Install Certificate** screen, paste the certificate into the **Certificate Text** field, or click **Select a File** to upload the certificate in a file.
   d. Click **Install**.

The installed certificate serial number of the device is updated on the controllers.

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, the device certificate state is shown as installed.

12. (Optional) Check the WAN Edge list on the controller to confirm that the device serial number is installed.

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number 12399910

                                                                HARDWARE
                                                                INSTALLED  SUBJECT
                SERIAL                                          SERIAL     SERIAL
CHASSIS NUMBER  NUMBER    VALIDITY  ORG                         NUMBER     NUMBER
-------------------------------------------------------------------------------
193A0122170001  18DB5D4F  valid     vIPtela Inc Regression      12399910   N/A
```

13. Remove the USB drive from the device.

Outcome

- The Cisco vEdge 5000 device is added to the overlay network and connected to the controllers using the SHA2 Enterprise Certificate.
- The device will use the installed SHA2 Enterprise Certificate after a reboot, a software upgrade, or a software downgrade to Cisco SD-WAN Release 20.3.1 or a later release. Use of SHA1 certificates is disabled.

Generate a Bootstrap File For Cisco IOS XE Catalyst SD-WAN Devices Using the CLI

To establish connectivity with the Cisco Catalyst SD-WAN controller, a device requires a minimum configuration. In most situations, this minimum bootstrap configuration (MBC) can be provided initially by plug-and-play (PnP). But in some situations, such as in remote sites where it may be preferable not to use PnP, it is helpful to have a saved bootstrap configuration that can connect the device to the controller.

The **request platform software sdwan bootstrap-config save** command saves the device configuration to the bootflash. The command can be used to save the configuration at any time, but it is intended for saving a minimum bootstrap configuration (MBC) file that enables the device to reconnect to the controller in case the full configuration is ever lost or removed.

When setting up a device, add to the configuration the details that are required to connect to the controller, and then use this command to save the MBC. The file is saved to this location:

bootflash:/ciscosdwan.cfg

Prerequisites

- The controller root certificate is installed on the Cisco IOS XE Catalyst SD-WAN device, to authenticate the device.
- The device is physically connected to the WAN through one of its interfaces.

Restrictions

- Onboarding using a bootstrap file does not support configuring cellular interfaces or other NIM module-specific configurations. If you need to configure these, push a full configuration after onboarding.
- Do not include policy configuration in the bootstrap file. If you need to configure policy, do this as part of a full configuration after onboarding.

Procedure

1. On the Cisco IOS XE Catalyst SD-WAN device, establish connectivity to Cisco SD-WAN Manager, by configuring the following:
    - System IP address
    - Domain ID
    - Site ID

- sp-organization-name
- organization-name
- Cisco SD-WAN Validator IP address and port number
- Tunnel with encapsulation configured as either GRE or IPSEC

Example:

```
system
system-ip 10.0.0.10
domain-id 1
site-id 200
admin-tech-on-failure
sp-organization-name CiscoISR
organization-name CiscoISR
vbond 10.0.100.1 port 12346
!
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet0/1/0
tunnel source GigabitEthernet0/1/0
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet0/1/0
tunnel-interface
encapsulation ipsec
exit
exit
commit
```

2. Use **show sdwan control connections** to verify connectivity to the Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.
3. Use the **request platform software sdwan bootstrap-config save** command to save a bootstrap file to the device bootflash.

   Example:

   ```
   Device#request platform software sdwan bootstrap-config save
   Saving bootstrap file 'bootflash:/ciscosdwan.cfg'...
   Done
   ```

   The configuration file is saved to this location:

   bootflash:/ciscosdwan.cfg

One Touch Provisioning: Onboard Cisco IOS XE Catalyst SD-WAN Devices Using Generic Bootstrap Configuration

Table 4: Feature History

Feature Name	Release Information	Description
One Touch Provisioning: Onboard Cisco IOS XE Catalyst SD-WAN Devices Using Generic Bootstrap Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	You can generate a generic bootstrap configuration on Cisco SD-WAN Manager and use this configuration to onboard multiple Cisco IOS XE Catalyst SD-WAN devices. When you boot a device with the generic bootstrap configuration, the device is listed on Cisco SD-WAN Manager as an unclaimed WAN edge device. To complete the onboarding, claim the device on Cisco SD-WAN Manager and attach a device template that configures the system IP address and site ID.

Overview of Generic Bootstrap Configuration

To onboard a Cisco IOS XE Catalyst SD-WAN device to the Cisco Catalyst SD-WAN overlay network, you generate a bootstrap configuration on Cisco SD-WAN Manager and boot the device with this configuration. After the device connects to Cisco SD-WAN Manager, you complete the onboarding using the Cisco SD-WAN Manager GUI. The bootstrap configuration contains device-specific configuration settings, requiring you to generate a bootstrap configuration for each device that you must onboard. From Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can use a generic bootstrap configuration to onboard multiple Cisco IOS XE Catalyst SD-WAN devices.

The generic bootstrap configuration omits device-specific details, such as the device UUID, and provides settings that a Cisco IOS XE Catalyst SD-WAN device can use to connect to the Cisco SD-WAN Validator. When the device connects to the Cisco SD-WAN Validator, the device is listed as an unclaimed WAN edge device on Cisco SD-WAN Manager. To complete the onboarding, you must claim the device on Cisco SD-WAN Manager and attach a device template that configures the system IP and site ID. Cisco SD-WAN Manager authenticates the device using a certificate that is installed on the device as part of the generic bootstrap configuration.

The generic bootstrap configuration contains the following:

- Organization name
- WAN interface to be enabled on the Cisco IOS XE Catalyst SD-WAN device
- IP address of the Cisco SD-WAN Validator
- Cisco SD-WAN Manager-signed certificate for authenticating the device.

To use generic bootstrap configuration to onboard a device, you must have a Dynamic Host Configuration Protocol (DHCP) server in the branch network where you are installing the device. The generic bootstrap configuration does not assign an IP address to the WAN interface. Instead, the configuration enables a DHCP client on the WAN interface so that the interface can acquire an IP address from a DHCP server in the branch network.

How the Generic Bootstrap Configuration Works

1. While generating the generic bootstrap configuration on Cisco SD-WAN Manager, you select the interface that will serve as the VPN 0 (WAN) interface on the Cisco IOS XE Catalyst SD-WAN device.
2. Copy the generic bootstrap configuration file onto the device bootflash and reset the device. On reset, the device is initialized with the generic bootstrap configuration.
3. The bootstrap configuration enables a DHCP client on the designated VPN 0 interface. The interface acquires an IP address and related details from a DHCP server in the network.
4. The device connects to the Cisco SD-WAN Validator through the VPN 0 interface is listed as an unclaimed WAN edge device on the Cisco SD-WAN Validator and Cisco SD-WAN Manager.
5. When you claim the device on Cisco SD-WAN Manager, Cisco SD-WAN Manager authenticates the device using the certificate installed on the device as part of the bootstrap configuration. After authentication, the device is listed among the valid WAN edge devices on Cisco SD-WAN Manager and the Cisco SD-WAN Validator.
6. Attach and push a template containing the system IP and site ID to the device.
7. The device establishes control connections to Cisco SD-WAN Controllers and is added to the overlay network.

Onboard a Cisco IOS XE Catalyst SD-WAN Device using Generic Bootstrap Configuration

1. Enable One Touch Provisioning:
   a. (Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier) From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
   b. Check if **One Touch Provisioning** is **Enabled**. If **Enabled**, go to Step 2.
   c. If **One Touch Provisioning** is **Disabled**, click **Edit**.
   d. For the **Enable Claim WAN Edges** setting, choose **Enabled** and click **Save**.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
3. Click **Export Bootstrap Configuration**.
   a. In the **Export Bootstrap Configuration** dialog box, enter the **VPN0 Interface name**.



Note The VPN 0 interface name may vary among Cisco IOS XE Catalyst SD-WAN device models. Specify the interface name based on the model you wish to onboard.

   b. Click **Generate Generic Configuration.**
4. Save the generic bootstrap configuration file.

   The file is named in the format `<filename>.cfg`.
5. Rename the generic bootstrap configuration file as `ciscosdwan.cfg`.
6. Copy the `ciscosdwan.cfg` file to a bootable USB drive or to the bootflash of the device.

7. If you are using a USB drive, plug the USB drive into the device.
8. Reset the device software configuration by issuing the following commands on the CLI:

```
Device# request platform software sdwan config reset
Device# reload
```



Note Performing a config reset generates a new type 6 master key. Therefore, ensure that the current password protecting the bootstrap configuration file is in plaintext and does not contain any type 6 keys. If the bootstrap configuration password contains type 6 keys, it will cause the device reset to fail.

9. Reboot the device.
   - While rebooting, the device reads the configuration file from the USB drive or the bootflash and applies the configuration.

     The configuration enables the VPN 0 interface and initializes a DHCP client on the interface. The interface acquires an IP address from a DHCP server in the network.

     The device connects to the Cisco SD-WAN Validator and is listed as an unclaimed WAN edge device on the Cisco SD-WAN Validator and Cisco SD-WAN Manager.
   - On the Cisco SD-WAN Validator, you can view the unclaimed WAN edge devices by using the command **show orchestrator unclaimed-vedges**.
   - In Cisco SD-WAN Manager, you can view the unclaimed WAN edge devices by selecting **Configuration** > **Devices** > **Unclaimed WAN Edges**.

     If the device is not listed as an unclaimed WAN edge device, check whether the device can connect to the Cisco SD-WAN Validator and correct any connectivity issues.
10. Claim the device on Cisco SD-WAN Manager:

    From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Unclaimed WAN Edges**.

    a. Choose the device you wish to claim and click **Claim Device(s)**.
       - The device is removed from **Unclaimed WAN Edges** and listed on **WAN Edge List**.
       - On the Cisco SD-WAN Validator, the device is listed as a valid WAN edge device. You can view the valid WAN Edge devices by issuing the command **show orchestrator valid-vedges**.
11. Attach a configuration template to the device.
    a. Ensure that the template includes the system IP address and the site ID.
    b. Push the template to the device.

Result

The device connects to Cisco SD-WAN Controllers and is added to the overlay network.

To verify that the device has established control connections and is part of the overlay network, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** and click the number in the **WAN Edges** area.

Note In Cisco vManage Release 20.6.x and earlier: To verify that the device has established control connections and is part of the overlay network, from the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** and click **WAN Edge** devices in the **Summary Pane**.

Remove a Cisco IOS XE Catalyst SD-WAN Device Onboarded Using Generic Bootstrap Configuration

1. Detach device from templates:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates** and select the template attached to the device.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

   c. For the selected template, click **...** and choose **Detach Devices**.
   d. In the **Available Devices** column, select the device to be detached from the template.
   e. Click the arrow pointing right to move the device to the **Selected Devices** column.
   f. Click **Detach**.

2. Connect to the device using SSH. From the device SSH terminal, shut down the VPN 0 WAN interface by using the following commands:

```
Device(config)# interface vpn0-interface-name
Device(config-if)# shutdown
```

3. Invalidate the device:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
   b. Click **WAN Edge List** and choose the device to invalidate.
   c. In the **Validate** column, click **Invalid**.
   d. Click **OK** to confirm the move to the invalid state.
   e. Click **Send to Controllers** to send the chassis and serial number of the invalidated device to the controllers in the network. Cisco SD-WAN Manager displays the **Push WAN Edge List** screen showing the status of the push operation.

4. Delete the WAN edge device:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. Click **WAN Edge List** and select the device you wish to remove.
   c. For the selected device, click **...** and choose **Delete WAN Edge**.
   d. Click **OK** to confirm deletion of the device.

Software Installation and Upgrade for Cisco IOS XE Routers

You can install up to two Cisco Catalyst SD-WAN images on the same router.

Supported Hardware Platforms and Interface Modules

For supported Hardware platforms and interface modules, see Release Notes.

Note For Cisco IOS XE Catalyst SD-WAN devices from Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, if a device boots using the .bin file after a PnP or auto-install process completes, the device comes up with its day-0 configuration. The device then reloads automatically and goes into install mode.

Supported Crypto Modules

The following crypto modules are required for the ASR 1000 series routers:

- ASR1001HX-IPSECHW, for the ASR 1001-HX
- ASR1002HX-IPSECHW, for the ASR 1002-HX

Before You Begin

Before you deploy an IOS XE router in the overlay network, review the following:

- The controller devices—Cisco SD-WAN Validators, Cisco SD-WAN Manager instances, and Cisco SD-WAN Controllers—are running Cisco Catalyst SD-WAN Software Release 18.3.
- If you deploy both IOS XE and vEdge routers in the overlay network, the vEdge routers are running Release 17.2.1 or higher of the Cisco Catalyst SD-WAN software. With these software versions, the vEdge and IOS XE software can interoperate, allowing BFD tunnels to be established between vEdge routers and IOS XE routers.
- If you deploy both IOS XE and vEdge routers in the same site, the vEdge routers are running Cisco Catalyst SD-WAN Software Release 18.3.
- The ISR 4000 series router has at least 4 gigabytes (GB) of DRAM installed. It is recommended that the router have 8 GB of DRAM.
- The ASR 1000 series router has at least 8 GB of DRAM installed. The ASR 1002-HX router has at least 16 GB of DRAM installed.
- The router bootflash has a minimum of 1.5 GB space available for the XE SD-WAN image or, beginning with Cisco IOX SD-WAN Release 17.10, the router bootflash has a minimum of one half of its disk space available for the XE SD-WAN image.
- If using your enterprise root certificate to authenticate the router, the certificate is copied to the router's bootflash before installing the XE SD-WAN software.
- All unsupported modules are removed from the router before installing the XE SD-WAN software. For a list of supported modules, see Supported Interface Modules and Supported Crypto Modules.

- For information about deploying a Cisco ASR 1006-X with an RP3 module, see Cisco ASR 1006-X with an RP3 Module.
- The updated device list is uploaded to Cisco SD-WAN Manager and sent to the Cisco SD-WAN Validator. To do so:
  1. Obtain the router's chassis and board ID serial number by issuing the **show crypto pki certificates CISCO_IDEVID_SUDI** command at the system prompt. If running Release 16.6.1 or earlier on an ASR series router, issue the **show sdwan certificate serial** command.
  2. Add the router's serial number to Plug and Play (PnP) Connect portal. See Add the IOS XE Router to the PnP Portal section for more details..
  3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**. Click **Sync Smart Account** to download the updated device list to Cisco SD-WAN Manager and send it to the Cisco SD-WAN Validator.
- Device configuration templates are created and attached to the router using Cisco SD-WAN Manager **Configuration** > **Templates**. This ensures that the router can obtain a configuration and establish full control connections when it comes up.
- If the router exceeds the unidirectional encrypted bandwidth of 250 Mbps and if the HSECK9 license is not already installed, the license file is copied to the router's bootflash and license installed on the router license install file path.
- The ASR 1000 series, ISR 1000 series, and ISR 4000 series router is running the required version of the ROM monitor software (ROMMON), as shown in the following table. To verify the ROMMON version running on the router, issue the **show rom-monitor** or **show platform** command at the system prompt.

Hardware Platform	Required ROM Monitor Software Version
ASR 1000 series	16.3 (2r)
ISR 1000 series	16.9 (1r)
ISR 4000 series	16.7 (3r)

- The ISRv router is running the minimum required version of the CIMC and NFVIS software, as shown in the following table:

Hardware Platform	CIMC	NFVIS
ISRv	3.2.4	3.8.1

Download Cisco IOS XE Catalyst SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier

Download the Cisco IOS XE Catalyst SD-WAN Software

To download the Cisco IOS XE Catalyst SD-WAN software from the Cisco site:

1. Go to https://www.cisco.com.
2. Click **Support & Downloads** from the menu on the left side.
3. In the **Products and Downloads** page, in the **Downloads** search box, choose Software-Defined WAN (SD-WAN).
4. In the **Select a Product** page, from the right-most pane, choose **XE SD-WAN Routers**.
5. From the right-most pane, select your router model.
6. Click the desired software release version to download it. The software image name has the format *router-model*-ucmk9.*release-number*
7. Copy the software image to an HTTP or FTP file server in your local network.

Install the Cisco IOS XE Catalyst SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier

All new Cisco IOS XE Catalyst SD-WAN devices ships with the Cisco IOS XE Catalyst SD-WAN software already installed.

If you have an existing Cisco IOS XE Catalyst SD-WAN device, follow these steps to install the Cisco IOS XE Catalyst SD-WAN software. The router reboots with the Cisco IOS XE Catalyst SD-WAN image.

1. Download the Cisco IOS XE Catalyst SD-WAN software image from the Cisco site.
2. Upload the Cisco IOS XE Catalyst SD-WAN software image from the file server to the bootflash of the device. Sample syntax for FTP is given below:

```
Device# (config)# ip ftp source-interface interface
Device# copyftp:// username:password@server-IP/file-location bootflash:
TFTP:
Device(config)# ip tftp source-interface interface
Device(config)# ip tftp blocksize 8192
Device(config)#exit
Device#copy tftp: bootflash:
SCP (assumes SSH is enabled):
Device# configure terminal
Device# (config)# ip scp server enable
FileServer$ scp filenameusername@router-IP:/filename
```

3. Ensure that the device is connected to a management console.
4. Create a backup of the current configuration that can be saved in the bootflash of the device.

```
Device# copy run bootflash:original-xe-config
```

5. Remove all existing boot statements and save the configuration.

```
ISR4K# (config)# no boot system ...
ISR4K# wr mem
```

6. Verify that the BOOT variable is blank in the following output.

```
ISR4K# show bootvar
BOOT variable =
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Standby not ready to show bootvar
```

7. Add a boot variable that points to the Cisco IOS XE Catalyst SD-WAN image.

```
Device(config)# boot system flash bootflash:
SDWAN-image
Device(config)# exit
ISR4K# write memory
```

8. Verify that the BOOT variable points to the Cisco IOS XE Catalyst SD-WAN image.

```
Device# show bootvar
BOOT variable =  bootflash:isr4300-ucmk9.16.10.1a.SPA.bin,1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exists
Configuration register is 0x2102
Standby not ready to show bootvar
```

9. Remove all existing configurations from the router.

```
Device# write erase
```

10. Set the config-register to 0x2102.

```
Device# configure terminal
Deovce(config)# config-register 0x2102
Device(config)# end
```

11. Verify that the config-register is set to 0x2102 or that it will be set to 0x2102 at the next reboot.

```
Device# show bootvar
```

12. Reboot the router.

```
ISR4K# reload
Proceed with reload? [confirm] Yes
If prompted to save the configuration, enter No. The router reboots with the XE SD-WAN
 image.
```

13. If prompted to enter the initial configuration dialog, enter **No**.

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [Yes/No]: No
```

14. If prompted to terminate auto-install, enter **Yes**.

```
Would you like to terminate auto-install? [Yes/No]: Yes
```

15. At the login prompt, log in with the default username and password as **admin**.

    The default password can be used once and then must be changed. If the initial configuration session times out or if the session is interrupted or terminated before the password is changed and saved, subsequent login attempts fail. To restore login access to the device, you must reset the password to its default value through the local console in ROMMON mode. Then the initial provision process must be restarted. For information about restoring the password, see Recover the Default Password, on page 57.

16. Stop PnP and allow the Cisco IOS XE Catalyst SD-WAN packages to install:

```
ISR4K# pnpa service discovery stop
```

17. Configure the upgrade on Cisco IOS XE Catalyst SD-WAN device using **request platform software sdwan software upgarde-confirm**.

```
Router# request platform software sdwan software upgrade-confirm
Router#
*Sep 21 00:26:29.242: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install commit PACKAGE
*Sep 21 00:26:30.153: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install commit PACKAGE
Router#
```

18. Ensure output of **show sdwan software** shows CONFIRMED state as user and no other value.

```
Router# sh sdwan software
VERSION       ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
--------------------------------------------------------------------------------
16.12.1b.0.4  true    true     true      user       2019-09-21T00:24:22-00:00

Total Space:388M Used Space:86M Available Space:298M
```

19. Configure the Cisco IOS XE Catalyst SD-WAN device using **request platform software sdwan software reset**.

```
Router# request platform software sdwan software reset

*Sep 21 00:27:20.025: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install activate bootflash:isr4300-ucmk9.16.12.1b.SPA.bin
*Sep 21 00:27:43.105: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
*Sep 21 00:28:47.233: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install activate PACKAGESep 21 00:28:54.240: %PMAN-5-EXITACTION: R0/0: pvp: Process
manager
```

Note Once you have installed this image, remember to use the command **config-transaction** to open CLI configuration mode. The **config terminal** command is not supported on Cisco Catalyst SD-WAN routers.

Note Downgrading to fresh install of old image versions is not supported. You can only downgrade to a previous existing version of old image. For example, if you have never installed Cisco IOS XE Catalyst SD-WAN 16.10.3 on your Cisco IOS XE Catalyst SD-WAN device, and if you try to downgrade from Cisco IOS XE Catalyst SD-WAN 16.11.1 release to Cisco IOS XE Catalyst SD-WAN 16.10.3 release then this operation is unsupported and results in unpredictable behavior. However, if you had a 16.10.3 image installed previously, then you could reactivate it by using the **request platform software sdwan activate** command.

Note Data is migrated from an existing Cisco Catalyst SD-WAN image to a new Cisco Catalyst SD-WAN image only during an upgrade. After an upgrade is completed, there is no migration of data between different versions of installed images for both Cisco IOS XE Catalyst SD-WAN and Cisco vEdge devices. For example, if you had installed 19.2.4 previously, and 20.3.2 is your current active image, then if you activate the 19.2.4 image, the additional configurations from 20.3.2 will not be migrated to 19.2.4.

Configure IOS XE Router Using CLI

If your Cisco IOS XE Catalyst SD-WAN device is connected to a DHCP server, PnP runs automatically and Cisco SD-WAN Manager automatically configures the device after the control connections are up. To verify that the control connections are up and the device is validated, enter the following command at the system prompt:

```
Device# show sdwan control connections
```

If your IOS Ex router is connected to a DHCP server and you are not using PnP, or if your IOS XE router is not connected to a DHCP server on the WAN, configure the router manually using the CLI as shown in the following steps.

You also can configure the hostname by using the **system host-name** *hostname* command. Configuring the hostname is optional, but it is recommended because this name in included as part of the prompt in the CLI and it is used on various Cisco SD-WAN Manager screens to refer to the device. This command is not available on the device CLI but it is available when using the CLI device template.

1. Connect to the router using a management console.
2. Stop PnP to allow access to the CLI:

   ```
   Device# pnpa service discovery stop
   ```
3. Enter configuration mode:

   ```
   Device# config-transaction
   Device(config)#
   ```
4. Configure the system IP address.

   ```
   Device(config-system)# system-ip  ip-address
   ```

   Cisco SD-WAN Manager uses the system IP address to identify the device so that the NMS can download the full configuration to the device.
5. Configure the numeric identifier of the site where the device is located:

   ```
   Device(config-system)# site-id site-id
   ```
6. Configure the IP address of the Cisco SD-WAN Validator or a DNS name that points to the Cisco SD-WAN Validator. The Cisco SD-WAN Validator's IP address must be a public IP address, to allow the router to reach the Cisco SD-WAN Validator.

   ```
   Device(config-system)# vbond (dns-name | ip-address)
   ```
7. Configure the organization name, which is the name that is included in the certificates on all devices in the overlay network. This name must be the same on all devices.

   ```
   Device(config-system)# organization-name name
   ```

8. Configure the tunnel interface to use for overlay connectivity. Ensure that the tunnel interface ID does not conflict with any other interface IDs that may be auto-assigned by Cisco SD-WAN Manager. You can verify this in configuration preview.

```
Device(config)# interface Tunnel #
Device(config-if)# ip unnumbered wan-physical-interface
Device(config-if)# tunnel source wan-physical-interface
Device(config-if)# tunnel mode sdwan
```

Note

- If you are using Cisco SD-WAN Manager **feature templates** for your configuration, a tunnel interface is automatically assigned based on the WAN interface used.
- If you switch to Cisco SD-WAN Manager **mode** from CLI mode, the tunnel interface you configured may change because Cisco SD-WAN Manager automatically assigns a tunnel interface number based on the WAN interface used. This change in tunnel number can cause the tunnel to go down before it comes up again when the configuration is pushed.

9. If the router is not connected to a DHCP server, configure the IP address of the WAN interface:

```
Device(config)# interface GigabitEthernet  #
Device(config)# ip address  ip-address mask
Device(config)# no shut
Device(config)# exit
```

10. Configure tunnel parameters:

```
Device(config)# sdwan
Device(config-sdwan)# interface  WAN-interface-name
Device(config-interface-interface-name)# tunnel-interface
Device(config-tunnel-interface)# color color/path-name
Device(config-tunnel-interface)# encapsulation  ipsec
```

11. If an IP address is manually configured on the router, configure a default route:

```
Device(config)# ip route 0.0.0.0 0.0.0.0 next-hop-ip-address
```

12. If the Cisco SD-WAN Validator address was defined as a hostname, configure DNS:

```
Device(config)# ip domain lookup
Device(config)# ip name-server dns-server-ip-address
```

13. Save the changes and exit configuration mode:

```
Device(config)# commit and-quit
Device# exit
```

14. If you are using a certificate signed by your enterprise root CA, install the certificate:

```
Device# request platform software sdwan root-cert-chain install bootflash: certificate
```

15. Verify that the control connections are up and the router is validated.

```
Device# show sdwan control connections

PEER    PEER PEER         SITE  DOMAIN  PEER         PEER PRIV  PEER        PEER PUB

TYPE    PORT SYSTEM IP    ID    ID      PRIVATE IP   PORT       PUBLIC IP   PORT
LOCAL COLOR
------------------------------------------------------------------------------------------
```

```
vsmart  dtls 192.168.1.2  10    1       172.1.1.3    12346      172.1.1.3   12346
 biz-internet
vbond   dtls -             0    0       172.1.1.4    12346      172.1.1.4   12346
 biz-internet
vmanage dtls 192.168.1.3  10    0       172.1.1.2    12346      172.1.1.2   12346
 biz-internet

                          CONTROLLER
                          GROUP
PROXY STATE  UPTIME       ID
-------------------------------------
  up         1:19:51:40   0
  up         1:19:51:45   0
  up         1:19:51:38   0
```

You can now configure SD-WAN features on the router using Cisco SD-WAN Manager templates.

Add IOS XE Devices to the Plug and Play Portal

Table 5: Feature History

Feature Name	Release Information	Description
On Premises ZTP Server for Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature extends the on-premise Plug and Play implementation support to Cisco IOS XE Catalyst SD-WAN routers.

To add a device to the Plug and Play portal:

- If the device can reach the PNP portal, see Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products.
- If the device does not have access to the PNP portal, see Start the Enterprise ZTP Server and Prepare Routers for ZTP sections in the Cisco Catalyst SD-WAN Overlay Network Bring-Up Process chapter.

Note When devices are due for Return Materials Authorization (RMA), the device details are with Cisco PNP. However, you cannot delete these devices from the RMA list in Cisco SD-WAN Manager. Instead Cisco SD-WAN Manager administrator can mark the devices returned as invalidated as per RMA.

For information abour Cisco IOS XE Release 17.2 and later, see Install and Upgrade Cisco IOS XE Release 17.2 and Later.

Upgrading or Downgrading ROMMON

This section describes how to upgrade or downgrade the ROM monitor (ROMmon) version that is running on a device. Perform this procedure if you need to change a ROMmon version to a required version that is shown in the “Before You Begin” section.

To determine the ROMmon version that is running on a device, enter the following command:

```
Device# Show rom-monitor R0
```

To upgrade or downgrade ROMmon, follow these steps:

1. Take either of these actions:
   a. Load the ROMmon file into the device bootflash using a method such as SCP, FTP, TFTP, or a USB drive.
   b. If you do not have out-of-band management access to the router, transfer the ROMmon file by using Cisco SD-WAN Manager CLI, as shown in the following example:

```
vManage# request execute vpn 0 scp -P 830 C1100-rommon-16-1r-SPA.pkg
admin@router-ip-address:/bootflash/vmanage-admin/C1100-rommon-169-1r-SPA.pkg
```

2. Take either of these actions to verify that the ROMmon file that you loaded or transferred appears in the directory output:
   a. If you loaded the ROMmon file into the device bootflash, enter the following command:

```
Device# dir bootflash
```

   b. If you transferred the ROMmon file by using the Cisco SD-WAN Manager CLI, enter the following command:

```
vManage# dir bootflash:vmanage-admin
```

3. Enter the following command to set config-register to 0x2102:

```
Device# config-register 0x2102
```

4. Upgrade (or downgrade) the ROMmon file on your device by using the upgrade command as shown in the following examples:
   - Example upgrade command if you loaded the ROMmon file into the device bootflash:

```
Device# upgrade rom-monitor filename bootflash: C1100-rommon-169-1r-SPA.pkg R0
```

   - Example upgrade command if you transferred the ROMmon file by using Cisco SD-WAN Manager CLI:

```
vManage# upgrade rom-monitor filename
bootflash:vmanage-admin/C1100-rommon-169-1r-SPA.pkg R0
```

5. After a series of messages pertaining to the upgrade display and the router prompt displays, enter the following command to reload the router:

```
Device# Reload
```

6. Enter the following command and verify that the output shows the new ROMmon version:

```
ISR4K# Show rom-monitor R0
```

Perform Factory Reset

This section describes the Factory Reset feature and how it can be used to protect or restore a router to an earlier fully functional state. For information on factory reset procedures on different platforms, see:

- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Cloud Services Router 1000V Series

Note To perform factory-reset on a Cisco IOS XE Catalyst SD-WAN ASR 1000 router, ensure that the router is booted in subpackages mode. Execute **show version** command and check the output for *system image file* to determine the booted image.

```
Device# show version
Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20200303_002119_V17_X_X_XX
Cisco IOS Software [Amsterdam], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Tue 03-Mar-20 00:29 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON

2KP-CEDGE uptime is 3 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:packages.conf"
```

Recover the Default Password

The default password for a Cisco IOS XE Catalyst SD-WAN device is admin. After using this password for the first time, the administrator must create a new password. If the initial configuration session times out or if the session is interrupted or terminated before a new password is created, subsequent login attempts fail. In this situation, you must recover the default password.

To recover the default password for a device, follow these steps:

1. Power the device down and then back up.
2. In the local console of the device, enter ROMMON mode.
3. Enter the following command to set the config-register value to 0x8000:

   ```
   rommon 1 > confreg 0x8000
   ```
4. Power the device down and then back up so that your update takes effect.
5. Log in to the device with the user name and the password as **admin**.
6. In the local console of the device, enter SD-WAN config mode.
7. Enter the following command to set the config-register value to 0x2102:

   ```
   Device# confreg 0x2102
   ```
8. In the local console of the device, enter privileged exec mode.
9. Take either of these actions:

- For Cisco IOS XE SD-WAN 16.10 releases beginning with release 16.10.4 or for Cisco IOS XE SD-WAN 16.12 releases beginning with release 16.12.2:

```
Device# request platform software sdwan config reset
Device# reload
```

- For Cisco IOS XE SD-WAN 16.10 releases earlier than release 16.10.4 or for Cisco IOS XE SD-WAN 16.12 releases earlier than 16.12.2:

```
Device# request platform software sdwan software reset
```

10. After the device comes back up, configure a new admin password.

Software Installation and Upgrade for vEdge Routers

This article describes how to install software on all Cisco vEdge devices—Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Control Componentss, Cisco SD-WAN Validators, and vEdge routers—and how to upgrade the software on devices already running the Cisco Catalyst SD-WAN software.

Software Image Signing

Cisco Catalyst SD-WAN software images are digitally signed to ensure that the images are official Cisco Catalyst SD-WAN images and to guarantee that the code has not been altered or corrupted since the image was created and signed. All standard Cisco Catalyst SD-WAN software images are signed, while patch images are not. Standard software images are identified with three numeric fields (such as 16.1.0) and patch software images are identified with four numeric fields (such as 16.1.0.1).

Signed images include a revocation mechanism so that Cisco Catalyst SD-WAN can revoke an image if it is found to be dangerous, either due to a bug or a security flaw. These revocation mechanisms protect from attacks if you attempt to install a previously signed image that has a known vulnerability.

After you have installed a signed imaged onto a Cisco Catalyst SD-WAN device, you can no longer install an unsigned image onto the device.

Software image signing is available in Releases 16.1 and later.

Software Version Compatibility

You can upgrade the software version on the controller devices—Cisco SD-WAN Manager instances, Cisco SD-WAN Controllers, and Cisco SD-WAN Validators—without upgrading the vEdge routers to the same version. However, the software version running on the controller devices must be compatible with the version running on the vEdge routers.

For a list of compatible versions on Controllers and vEdge routers, see Release Notes.

Note All controller devices of the same type must run the same software version. That is, all Cisco SD-WAN Manager instances must run the same software version, all Cisco SD-WAN Controllers must run the same software version, and all Cisco SD-WAN Validators must run the same version.

Install the Software

Before you begin, download the software from the Cisco Catalyst SD-WAN Support site.

You install software on Cisco Catalyst SD-WAN devices when you first bring up the overlay network and add those devices to the network:

- To install software on a Cisco SD-WAN Validator, see *Create Cisco SD-WAN Validator VM Instance on ESXi* or *Create Cisco Catalyst SD-WAN Validator VM Instance on KVM*. During the process of creating the VM, you install the vBond.ova file.
- To install software on a vEdge Cloud router, see *Create vEdge Cloud VM Instance on AWS*, *Create vEdge Cloud VM Instance on ESXi*, or *Create vEdge Cloud VM Instance on KVM*. During the process of creating the VM, you install the vEdge Cloud.ova file.
- To install software on a Cisco SD-WAN Manager, see *Create Cisco SD-WAN Manager VM Instance on ESXi* or *Create Cisco SD-WAN Manager Instance on KVM*. During the process of creating the VM, you install vManage.ova file.
- To install software on a Cisco Catalyst SD-WAN Controller, see *Create Cisco Catalyst SD-WAN Controller VM Instance on ESXi* or *Create Cisco Catalyst SD-WAN Controller VM Instance on KVM*. During the process of creating the VM, you install the vSmart.ova file.
- To install software on a hardware vEdge router, nothing is required. All vEdge hardware routers ship with the software already installed.

Upgrade the Software

From Cisco SD-WAN Manager, you can upgrade the software image running on a Cisco vEdge device in the overlay network and reboot it with the new software. You can do this for a single device or for multiple devices simultaneously.

To upgrade the software, you obtain the software images from Cisco Catalyst SD-WAN, add the new software images to the repository located on either Cisco SD-WAN Manager or a remote server, and install the new software image on the device. The next reboot occurs immediately if you select the **Activate and Reboot** check box, or you can wait until the next regularly scheduled maintenance window. If an upgrade fails and the device does not come back up, Cisco SD-WAN Manager automatically reverts the device to the previously running software image.

Before you upgrade the software on Cisco vEdge devices, ensure that the devices are running the required software version.

Note Cisco Catalyst SD-WAN releases starting with Releases 18.4.5, 19.2.2, and 20.1.1 have a security lockout. When any of these software versions (or later) are installed and activated on a device, a 30-day timer is set for the removal of any old images that were previously installed on the device. After the timer expires, the old images are deleted. For example, if you install and activate Release 18.4.5, a 30-day timer starts on the previously installed Release 19.2.1 image, but not on Release 19.2.2. Similarly if you install and activate Release 19.2.2, a 30-day timer starts on the previously installed Release 18.4.4 image, but not on Release 18.4.5.

You can continue to activate an older image that is already installed, before the 30-day timer runs out. If the device restarts before the 30-day timer expires, the timer is reset.

See Cisco Catalyst SD-WAN Command Reference guide for more information.

- **request software secure-boot set**- Makes the system immediately delete old images* without waiting the 30 days.
- **request software secure-boot status**- Displays the installed old images*.
- **request software secure-boot list**- Prints a list of all old images* that are installed.

*old images= before releases 18.4.5, 19.2.2, and 20.1.1

Note Cisco SD-WAN Manager downgrade is not supported. Ensure that you take a snapshot of the VM prior to upgrading Cisco SD-WAN Manager. To rollback to an earlier Cisco SD-WAN Manager release, revert to the snapshot.

For additional information and caveats regarding software upgrades, see Release Notes.

Best Practices for Software Upgrades

- Upgrade the software from Cisco SD-WAN Manager rather than from the CLI.
- If you are upgrading the software image on a remote Cisco SD-WAN Manager, the overlay network must already be up and operational.
- If you are upgrading all devices in the overlay network, you must perform the upgrade in the following order:
  1. Upgrade Cisco SD-WAN Manager instances.
  2. Upgrade the Cisco SD-WAN Validators.
  3. Upgrade one-half of the Cisco SD-WAN Controllers.
  4. Have the upgraded Cisco SD-WAN Controllers run for at least one day (24 hours) to ensure that the Cisco vEdge devices and the overlay network are stable and running as expected.
  5. Upgrade the remainder of the Cisco SD-WAN Controllers.
  6. Upgrade 10 percent of the vEdge routers. For multirouter sites, it is recommended that you upgrade only one router per site.

7. Have the upgraded vEdge routers run for at least one day (24 hours) to ensure that the Cisco Catalyst SD-WAN devices and the overlay network are stable and running as expected.
8. Upgrade the remainder of vEdge routers.



Note From Cisco Catalyst SD-WAN Control Components Release 20.13.1, for a Cisco vEdge device, the control session rate for Datagram Transport Layer Security (DTLS) increases to 4000 pps only for the duration of upgrade and is reset to the original value after the upgrade is complete.

- If the new software images are located on an FTP server, ensure that the FTP server can handle concurrent file transfers.
- If the new software images are in the image repository on Cisco SD-WAN Manager, ensure that the WAN in which Cisco SD-WAN Manager is located has sufficient capacity for concurrent file transfers.
- You cannot include Cisco SD-WAN Manager in a group software upgrade operation. You must upgrade and reboot Cisco SD-WAN Manager server by itself.
- In a group software upgrade operation, you can upgrade up to 40 Cisco vEdge devices or Cisco IOS XE Catalyst SD-WAN devices and reboot or activate upto 100 Cisco vEdge devices or Cisco IOS XE Catalyst SD-WAN devices simultaneously (when the new image is available locally). These maximum numbers assume that Cisco SD-WAN Manager is idle and only upgrade and reboot operations are being carried out. In case of other management tasks occuring on Cisco SD-WAN Manager at the same time, the number of available sessions reduces.
- When you are setting a software image to be the default software image, activate it first, before making it the default image.
- If you re-activate a previously activated image after making the configuration changes, unexpected behavior may occur due to differences in the configuration. You must perform fresh installation and activation of a new software version.

Obtain Software Images from Cisco Catalyst SD-WAN

To upgrade the software running on the devices in the overlay network, you must first obtain the new software packages from the Cisco Catalyst SD-WANwebsite. To do so, go to http://www.cisco.com/go/support, log in to Cisco Catalyst SD-WAN Support, and download the software packages for the new release. You can also download the software images to an FTP server in your network and, from Cisco SD-WAN Manager, point to the upgrade packages on the remote host.

For initial software installation, the software package names for Releases 16.1 and later have the following format, where *x.x.x* represents the Cisco Catalyst SD-WAN software release version. These packages contain the virtual machines and the Cisco Catalyst SD-WAN software.

- vEdge Cloud router
  - viptela-*x.x.x*-edge-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-edge-genericx86-64.qcow2 (for KVM Hypervisor)

- Cisco SD-WAN Validator
  - viptela-edge-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-edge-genericx86-64.qcow2 (for KVM Hypervisor)
- Cisco Catalyst SD-WAN Controller
  - viptela-smart-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-smart-genericx86-64.qcow2 (for KVM Hypervisor)
- Cisco SD-WAN Manager
  - viptela-vmanage-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-vmanage-genericx86-64.qcow2 (for KVM Hypervisor)

The software upgrade package names for Releases 16.1 and later have the following format, where *x.x.x* represents the release version. The strings mips64 and x86_64 represent the underlying chip architecture.

- vEdge router hardware—viptela-*x.x.x*-mips64.tar.gz
- Cisco SD-WAN Validator, vEdge Cloud router, and Cisco Catalyst SD-WAN Controller—viptela-*x.x.x*-x86_64.tar.gz
- Cisco SD-WAN Manager—vmanage-*x.x.x*-x86_64.tar.gz

For Releases 15.4 and earlier, the software upgrade packages are in files with the extension .tar.bz2, or in the case of the vEdge 100 router, .tar.gz. The package names have the following format, where *x.x.x* represents the release version. The strings mips64 and x86_64 represent the underlying chip architecture.

- vEdge router—viptela-*x.x.x*-mips64.tar.bz2
- Cisco SD-WAN Validator and Cisco Catalyst SD-WAN Controller—viptela-*x.x.x*-x86_64.tar.bz2
- Cisco SD-WAN Manager—vmanage-*x.x.x*-x86_64.tar.bz2

Add New Software Images to the Repository

Once you have downloaded the new software packages from the Cisco Catalyst SD-WAN website, upload them into Cisco SD-WAN Manager repository. If you downloaded the software images to an FTP server, from Cisco SD-WAN Manager, point to the upgrade packages on the remote host.

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2.
3. Click **Add New Software**, and select the location from which to download the software image. The location can be:
   - Cisco SD-WAN Manager—To select an image stored on the local Cisco SD-WAN Manager.
   - Remote Server (preferred) —To select an image stored on a remote file server.
   - Remote Server – Cisco SD-WAN Manager—To select an image stored on a remote Cisco SD-WAN Manager. This location is available in Releases 17.2 and later.

4. If you select Cisco SD-WAN Manager, the Upload Software to Cisco SD-WAN Manager dialog box opens.
   a. Click **Browse** to select the software images or **Drag and Drop** the images for vEdge routers, Cisco SD-WAN Controllers, or Cisco SD-WAN Manager.
   b. Click **Upload** to add the images to Cisco SD-WAN Manager repository.
5. If you select Remote Server, the Location of Software on Remote Server dialog box opens.
   a. Enter the version number of the software image.
   b. Enter the URL of the FTP or HTTP server on which the images reside.
   c. Click **OK** to point to the software images on the remote host.
6. If you select Remote Server – Cisco SD-WAN Manager, the Upload Software to Cisco SD-WAN Manager dialog box opens.
   a. Enter the hostname of the Cisco SD-WAN Manager server.
   b. Click **Browse** to select the software images or **Drag and Drop** the software image for vEdge routers, Cisco SD-WAN Controllers, or Cisco SD-WAN Manager.
   c. Click **Upload** to add the images to Cisco SD-WAN Manager repository.

The added software images are listed in Cisco SD-WAN Manager repository table and are available for installing on the devices. The table displays the name and type of image, when it was updated, and the URL.

For the desired software version, click **...** and select **Delete** to delete the software version added to the list.

Upgrade the Software Image

After the software images are present in Cisco SD-WAN Manager image repository, you can upload the software image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click the check box and select one or more devices on which to upgrade the software image. To search for a device, use the **Device Groups** drop-down and/or the Search box.
3. Click **Upgrade** and the Software Upgrade dialog box opens.
4. From the **Version** drop-down, select the version of the software image you want to install. Cisco SD-WAN Manager and Remote Server are activated.
5. Select whether the software image is available on Cisco SD-WAN Manager or on the Remote Server.
6. If you select Remote Server in Step 5, choose the appropriate VPN for Cisco Catalyst SD-WAN Controller/Cisco SD-WAN Manager and for vEdge, and continue with Step 8.
7. If you select Cisco SD-WAN Manager in Step 5, you can choose to automatically activate the new software image and reboot the device by selecting the **Activate and Reboot** check box. (Note that if you do not select the **Activate and Reboot** check box, the new software image is still installed but the device continues to use the existing software image. To activate the newly installed software image, see Activate a New Software Image below.)

8. Click **Upgrade**. A progress bar indicates the status of the software upgrade.

If the upgrade does not complete successfully within 60 minutes, it times out.

If the control connection to Cisco SD-WAN Manager does not come up within 15 minutes, Cisco SD-WAN Manager automatically reverts the device to the previously running software image.

Activate a New Software Image

If you select **Activate and Reboot** check box when uploading the software image, then when you click **Upgrade**, the new software activates automatically and the device reboots.

If you uploaded the software image from a Remote Server, or if you did not select **Activate and Reboot** check box when uploading the software image from Cisco SD-WAN Manager, the new image is installed on the device but the device continues to use the existing software image. To activate the new software image:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click the check box to select one or more devices on which to activate the new software image. To search for a device, use the **Device Groups** drop-down and/or the Search box.
3. Click **Activate** to activate the new software. The activation process reboots the device and upgrades it to the newly installed software.

If the control connection between the device and Cisco SD-WAN Manager does not come up within 15 minutes, Cisco SD-WAN Manager automatically reverts the device to the previously running software image.

View Log of Software Upgrade Activities

To view the status of software upgrades on each device and a log of related activities:

1. Click the **Active Devices** toggle button. The top of the screen, directly below the title bar, displays the total number of upgrades performed along with the total number of successes and failures. The Software Upgrade table displays the status of each upgrade operation.
2. Click the right angle bracket to the left of each table row to see details of the operation. To close the details, click the down angle bracket.

Upgrade a Software Image from the CLI

If you need to upgrade a software image directly on a device, or if you are not using Cisco SD-WAN Manager in your network, to upgrade the software image, you can either repeat the installation process or you can install the software image from within the CLI.

To upgrade the software image from within the CLI:

1. Configure the time limit for confirming that a software upgrade is successful. The time can be from 1 through 60 minutes.

   ```
   Device# system upgrade-confirmminutes
   ```

2. Install the software:

   ```
   vEdge# request software install  url
   /viptela- release -mips64.tar.bz2 [reboot] [vpn vpn-id]
   ```

```
vSmart# request software install url/viptela- release
-x86 _64.tar.bz2 [reboot] [vpn vpn-id]
```

Specify the image location in one of the following ways:

- The image file is on the local server:

  /*directory-path*/

  You can use the CLI's autocompletion feature to complete the path and filename.

- The image file is on an FTP server.

  ftp://*hostname*/

- The image file is on an HTTP server.

  http://*hostname*/

- The image file is on a TFTP server.

  tftp://*hostname*/

Optionally, specify the VPN identifier in which the server is located.

The **reboot** option activates the new software image and reboots the device after the installation completes.

3. If you did not include the **reboot** option in Step 2, activate the new software image and reboot the device:

   ```
   Viptela# request software activate
   ```

4. Confirm, within the configured upgrade confirmation time limit, that the software upgrade was successful:

   ```
   Viptela# request software upgrade-confirm
   ```

   If you do not issue this command within this time limit, the device automatically reverts to the previous software image.

Redundant Software Images

You can download and store multiple software images on a Cisco vEdge device.

To list the currently installed software version and to see which software image is currently running, use the following command:

```
Viptela# show software
VERSION   ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
15.4.3    true    false    false     user       2016-02-04T03:45:13-00:00
15.4.2    false   true     true      user       2015-12-06T14:01:12-00:00
```

To upgrade the software to a specific version, use the following command:

```
Viptela# request software activate
```

Downgrade a Cisco vEdge Device to an Older Software Image

To downgrade a Cisco vEdge Device to a previous software image using CLI:

1. If necessary, remove an existing software image to provide space for loading a new software image.

```
vEdge# request software remove  previous-installed-build
```

2. Download the software image for the downgrade.
3. Install the downloaded image.

   ```
   vEdge# request software install desired-build
   ```

   We recommend copying the image to local storage before installing, but you can specify the image location in one of the following ways:

   - The image file is on the local server:

     /*directory-path*/

     You can use the CLI's autocompletion feature to complete the path and filename.

   - The image file is on an FTP server.

     ftp://*hostname*/

   - The image file is on an HTTP server.

     http://*hostname*/

   - The image file is on a TFTP server.

     tftp://*hostname*/

4. Set the installed image as the default.

   ```
   vEdge# request software set-default desired-build
   ```

5. Perform a reset. This resets the device, deleting any existing configuration. The device starts in day zero configuration.

   ```
   vEdge# request software reset
   ```

Upgrade Memory and vCPU Resources on a Virtual Machine Hosting Cisco Catalyst SD-WAN Manager

Perform the following steps to upgrade the memory and virtual central processing unit (vCPU) resources on a virtual machine (VM) hosting Cisco SD-WAN Manager.

Note Only memory or vCPU increase is allowed. After the memory or vCPU is upgraded, you cannot downgrade.

1. Check the current configuration on Cisco SD-WAN Manager using the command **show system status**.

   ```
   vManage#show system status

   Viptela (tm) vmanage Operating System Software
   Copyright (c) 2013-2021 by Viptela, Inc.
   Controller Compatibility:
   Version: 20.7.0-185
   Build: 185
   ```

```
System logging to host  is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up
System FIPS state:       Enabled
Testbed mode:            Enabled
Engineering Signed:      True

Last reboot:             Initiated by user.
CPU-reported reboot:     Not Applicable
Boot loader version:     Not applicable
System uptime:           1 days 02 hrs 44 min 52 sec
Current time:            Sat Oct 23 22:12:10 UTC 2021

Load average:            1 minute: 14.58, 5 minutes: 12.31, 15 minutes: 10.73
Processes:               5775 total
CPU allocation:          32 total
CPU states:              31.58% user,   4.36% system,   64.06% idle
Memory usage:            65741448K total,    38096172K used,   490324K free
                         4606444K buffers,  22548508K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       15230M  3496M  10898M   24%   /
vManage storage usage:   Filesystem      Size  Used  Avail  Use%  Mounted on
                         /dev/sdb        502942M  206906M  270435M   41%   /opt/data

Personality:             vmanage
Model name:              vmanage
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
Chassis serial number:   None
```

2. Power the device down to upgrade the memory.
3. Upgrade the CPU and memory for the VM using the guidelines of the hosting platform. You can make the following upgrades:

Resources	Current	Upgrade
vCPU	16	32
Memory	32 G	64 G or 128 G
Memory	64 G	128 G

4. Power on the device and verify the memory and CPU.

```
vManage1# show system status

Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
Version: 20.7.0-139
Build: 139


System logging to host  is disabled
System logging to disk is enabled
```

```
System state:            GREEN. All daemons up
System FIPS state:       Enabled
Testbed mode:            Enabled
Engineering Signed:      True

Last reboot:             Initiated by user - activate 20.7.0-139.
CPU-reported reboot:     Not Applicable
Boot loader version:     Not applicable
System uptime:           16 days 17 hrs 43 min 28 sec
Current time:            Sat Oct 23 22:22:16 UTC 2021

Load average:            1 minute: 15.86, 5 minutes: 13.02, 15 minutes: 11.45
Processes:               6067 total
CPU allocation:          32 total
CPU states:              32.13% user,   4.34% system,   63.53% idle
Memory usage:            131703148K total,    88221488K used,   19285636K free
                         7022488K buffers,  17173536K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       15998M  10702M  4461M   71%   /
vManage storage usage:   Filesystem      Size  Used  Avail  Use%  Mounted on
                         /dev/sdb        10402115M  702212M  9175615M   6%   /opt/data

Personality:             vmanage
Model name:              vmanage
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
Chassis serial number:   None
```

Expand the secondary disk size, Cisco Catalyst SD-WAN Manager Release 20.12.x and later

Perform these steps to increase the size of the secondary disk on the virtual machine hosting a Cisco SD-WAN Manager instance.

Before you begin

For Cisco Catalyst SD-WAN Manager Release 20.13.x and later releases, this procedure is not effective. Redeploy the SD-WAN Manager virtual machine to correct the secondary disk size. Contact the Cisco TAC team for assistance with the redeployment procedure for your environment.

Procedure

Step 1 Shut down the virtual machine hosting Cisco SD-WAN Manager.

Step 2 Using the hypervisor (for example, ESXi, Azure, or AWS), provision additional space for the secondary disk of the virtual machine hosting Cisco SD-WAN Manager.

Step 3 Restart the VM that is hosting Cisco SD-WAN Manager.

Step 4 In Cisco SD-WAN Manager, enter the following to enable Cisco SD-WAN Manager to detect the additional disk space and extend the file system to use the space.

```
vm# request nms application-server resize-data-partition
```

Step 5 Enter the following commands to confirm that the /opt/data disk has been resized.

```
vm# vshell
vm:~$ df -hk | grep data
```

The output shows the new disk size.

Software Maintenance Upgrade for Cisco IOS XE Catalyst SD-WAN Devices

Table 6: Feature History

Feature Name	Release Information	Description
Support for Software Maintenance Upgrade Package	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables support for a Software Maintenance Upgrade (SMU) package that can be installed on Cisco IOS XE Catalyst SD-WAN devices. The SMU package provides a patch fix or a security resolution to a released Cisco IOS XE image. Developers can build this package that provides a fix for a reported issue without waiting for the fix to become available in the next release.
SMU Support for Cisco ISR1100 and ISR1100X Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	Added support for Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers.

Information About Software Maintenance Upgrade

A software maintenance upgrade (SMU) is a point fix for a critical bug in released software that attempts to minimize disruption to the router, if possible. An SMU is not designed to replace a maintenance release.

Cisco provides SMU fixes as package files, a file for each release and each component of Cisco Catalyst SD-WAN. The package contains metadata that describes the content of the package and the fix for a reported issue.

SMU Image Files

Each SMU image filename in the software repository includes a base image version and the defect ID related to the fix. In the image name:

- *base_image_version* is the Cisco IOS XE image version.
- *defect_id* is the identifier of the defect for which the SMU package has the fix.

SMU Types

An SMU type describes the effect of an installed SMU package on a Cisco IOS XE Catalyst SD-WAN device. The following are the SMU package types:

- Hot SMU (non-reload): Enables an SMU package to take effect after an SMU image activation without rebooting (reloading) the Cisco IOS XE Catalyst SD-WAN device.
- Cold SMU (reload): Enables an SMU package to take effect after rebooting (reloading) the Cisco IOS XE Catalyst SD-WAN device.

Benefits of Software Maintenance Upgrades

- Allow you to address a network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE Catalyst SD-WAN device internally validates the SMU image compatibility and does not allow you to install non-compatible SMU packages.
- Allow you to install or activate only one SMU package on devices at a time to simplify the initial implementation process.
- Allow you to install an SMU package on multiple Cisco IOS XE Catalyst SD-WAN devices at the same time when installing using Cisco SD-WAN Manager. To install an SMU package on multiple devices using the CLI, ensure that you repeat the install process on multiple devices.

Supported Devices for Software Maintenance Upgrade

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.9.5a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.9.x Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and later	• Cisco ISR 1000 Series Integrated Services Routers • Cisco IR1101 Integrated Services Router Rugged • Cisco ISR 4000 series Integrated Services Routers • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Series Edge Platforms • Cisco Catalyst 8000v Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x	• Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200L Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x	Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers

Manage Software Maintenance Upgrade Images

Use Cisco SD-WAN Manager to add, upgrade and activate, or deactivate and remove an SMU image.

Note When you activate or deactivate an SMU image, the device may reboot, depending on the SMU image. A non-reload SMU type does not trigger a device reboot; a reload SMU type triggers a device reboot.

Add, View, and Activate an SMU Image

1. Add an SMU image using the Cisco SD-WAN Manager software repository.

   See the Cisco SD-WAN Manager Add Software Images to Repository procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

2. View SMU images using the Cisco SD-WAN Manager software repository.

   See theCisco SD-WAN Manager View Software Images procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*. Note the following points when viewing SMU images:

   - The **Available SMU Versions** column displays the number of SMU images available for the current base image version (Cisco IOS XE image version).
   - View the defects that are associated with an SMU image by clicking a desired entry in the **Available SMU Versions** column. In the **Available SMU Versions** dialog box, you can view the defect ID, the corresponding SMU version, and the SMU types, such as non-reload or reload.
   - In the **Available SMU Versions** dialog box, delete an SMU version by clicking the delete icon next to an SMU version.

3. Upgrade an SMU image using the Cisco SD-WAN Manager software upgrade window.

   See the Cisco SD-WAN Manager Upgrade the Software Image on a Device procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*. Note the following points about the SMU image that you choose to upgrade:

   - In the devices table, the **Available SMUs** column displays the number of SMU images that are available for the current base image version.
   - View a list of all available SMU versions and the upgrade images for a device by clicking a desired entry under the **Available SMUs** column. In the **Available SMUs** dialog box, you can view the SMU versions, SMU types, and the state of an SMU version.

     The SMU version is in the format *base_image_version.cdet_id*.

   - In the **Upgrade** dialog box, optionally check **Activate and Reboot** to activate an SMU image and perform a reboot of the Cisco IOS XE Catalyst SD-WAN device automatically.

     After you check the **Activate and Reboot** check box, Cisco SD-WAN Manager installs and activates the SMU image on a device and triggers a reload based on the SMU type. For more Information about activating a software image, see the Cisco SD-WAN Manager Activate a Software Image procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

   After a successful upgrade of an SMU image, the Cisco IOS XE Catalyst SD-WAN device sends a corresponding success message.

Deactivate or Remove an SMU Image

Deactivate an SMU image and remove the image from a device using the Delete a Software Image procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Onboarding ISR1100 to Cisco SD-WAN Manager

1. Do not enable the Cisco IOS XE Catalyst SD-WAN device interface on the ISR1100 device.
2. Add the serial.viptela file to Cisco SD-WAN Manager to add the device.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Migrate Device** to migrate from viptela operating system to Cisco IOS XE operating system.
4. Enable the Cisco IOS XE Catalyst SD-WAN device interface to bring up the control connections.
5. Verify the device sync up in Cisco SD-WAN Manager.

Manage Software Maintenance Upgrade Images Using the CLI

Use the following CLIs to install, upgrade and activate, or deactivate and remove an SMU image.

Note When an SMU image is activated and deactivated, the device reboot may be triggered based on non-reload or reload SMU types. A non-reload SMU type does not trigger a device reboot, but a reload SMU type triggers a device reboot.

Install and Activate an SMU Image Using the CLI

1. Upload the SMU image from the file server to the bootflash of the device.

   Use the `copy` command to upload an SMU image. For information about the copy command, see Step 2 of the Install the Cisco IOS XE Software topic.

2. If not already configured, configure the time limit for confirming that a SMU image activation is successful.

   The time limit can be 1 through 60 minutes. We recommend that you configure the time limit to be at least 15 minutes.

   ```
   Device# config-transaction
   Device(config)# system
   Device(config-system)# upgrade-confirm minutes
   ```

3. Install an SMU image from the bootflash of your device and perform a compatibility check for the device and SMU package version.

   ```
   Device# request platform software sdwan smu install file-path
   ```

4. Activate the SMU image on a Cisco IOS XE Catalyst SD-WAN device.

   ```
   Device# request platform software sdwan smu activate build-number.smu-defect-id
   ```

5. Confirm the upgrade of the SMU image within the configured confirmation time limit.

   ```
   Device# request platform software sdwan smu upgrade-confirm
   ```

Note If you don't issue this command on the device within the time limit that is specified in the **upgrade-confirm** *minutes* command, the device automatically reverts to the state that it was in before the SMU image activation.

Deactivate and Remove an SMU Image Using the CLI

1. If not already configured, configure the time limit for confirming that a SMU image deactivation is successful.

   The time limit can be 1 through 60 minutes. We recommend that you configure the time limit to at least 15 minutes.

   ```
   Device# config-transaction
   Device(config)# system
   Device(config-system)# upgrade-confirm minutes
   ```

2. Deactivate an SMU image on a Cisco IOS XE Catalyst SD-WAN device.

   ```
   Device# request platform software sdwan smu deactivate
   build-number.smu-defect-id
   ```

3. Confirm that the SMU image can be deactivated.

   ```
   Device# request platform software sdwan smu upgrade-confirm
   ```

Note If you do not issue this command on the device within the time limit specified in the **upgrade-confirm** *minutes* command, the image deactivation fails and the device automatically reverts to the state that it was in before the SMU image deactivation.

4. Remove an SMU image from a Cisco IOS XE Catalyst SD-WAN device.

   ```
   Device# request platform software sdwan smu remove build-number.smu-defect-id
   ```

The following examples show commands that you can use to manage the SMU image operations.

- Check the upgrade and confirm the configuration:

  ```
  show sdwan running system
  ```

- Add and upgrade the confirm timer:

  ```
  config-transaction
  system
  upgrade-confirm 15
  commit
  ```

- Execution commands:

  - `request platform software sdwan smu install bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin`
  - `request platform software sdwan smu activate 17.09.01a.0.247.CSCvq24042`
  - `request platform software sdwan smu upgrade-confirm`

- **request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042**
- **request platform software sdwan smu upgrade-confirm**
- **request platform software sdwan smu remove 17.09.01a.0.247.CSCvq24042**

Verify Status of Software Maintenance Upgrade Images

You can monitor the status of the SMU image by using Cisco SD-WAN Manager or the CLI.

Monitor SMU Status Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. For the desired Cisco IOS XE Catalyst SD-WAN device, click an SMU image link (hyperlink) under **Available SMUs**.

   In the **Available SMUs** dialog box, you can view the state of an SMU image.

If no SMU images are available for the current base image version (Cisco IOS XE image version), the SMU image link is not available under **Available SMUs** and Cisco SD-WAN Manager displays 0.

Verify SMU Status Using the CLI

Example 1:

The following is a sample output from the **show install summary** command after installing, activating, and confirming the upgrade (committed) of an SMU image.

```
Device# show install summary[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01a.0.247
SMU   I   bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin


--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

The output shows that an SMU image is installed and activated from the bootflash file system. You can track the time that is left for rollback of an SMU image from the `Auto abort timer` value. This value displays the time that is left for the `Auto abort timer` to expire and the device to roll back.

Example 2:

The following example shows the output after using the **request platform software sdwan smu deactivate** command to deactivate an SMU image.

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042
smu_deactivate: START Mon Mar 5 21:54:06 PST 2021
smu_deactivate: Deactivating SMU
Executing pre scripts....

Executing pre scripts done.
```

```
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on all members
  [1] SMU_DEACTIVATE package(s) on switch 1
  [1] Finished SMU_DEACTIVATE on switch 1
Checking status of SMU_DEACTIVATE on [1]
SMU_DEACTIVATE: Passed on [1]
Finished SMU Deactivate operation
SUCCESS: smu_deactivate 17.09.01a.0.247.CSCvq24042
```

The output shows that an SMU image is deactivated from the device.

The following is a sample output from the **show install summary** command after deactivating an SMU image.

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------

IMG   C    17.09.01a.0.247
SMU   D    bootflash: c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 00:04:57
--------------------------------------------------------------------------------
```

The following sample output shows the output of deactivating an SMU image after confirming that the SMU image can be deactivated using the **request platform software sdwan smu upgrade-confirm command**.

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042

install_deactivate: START Thu Aug 25 17:47:10 UTC 2022
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on Active/Standby
  [1] SMU_DEACTIVATE package(s) on R0
  [1] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation

CSCvq24042:SUCCESS
SUCCESS: install_deactivate /bootflash/c8kv_hot.bin Thu Aug 25 17:47:33 UTC 2022
```

The following is a sample output from the **show install summary** command after removing an SMU image.

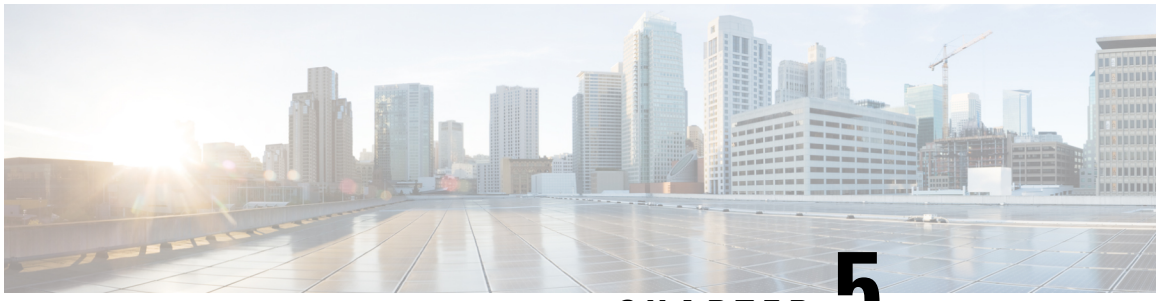
```
Device# show install summary[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01a.0.247

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Example 3:

The following is a sample output from the **show install package** command to view the metadata of an SMU image such as, SMU type, SMU ID, SMU defect ID, and so on.

```
Device# show install package
bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
Name: c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
Version: 17.09.01a.0.247.1660805065
Platform: C8000V
Package Type: SMU
Defect ID: CSCvq24042
Package State: Inactive
Supersedes List: {}
SMU Fixes List: {}
SMU ID: 24042
SMU Type: non-reload
SMU Compatible with Version: 17.09.01a.0.247
SMUImpact:
```



CHAPTER 5

Cisco SD-AVC

- Cisco SD-AVC feature history, on page 77
- Cisco SD-AVC, on page 77
- Cloud-hosted SD-AVC service, on page 78
- Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later, on page 79
- Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier, on page 81

Cisco SD-AVC feature history

Table 7: Feature History

Feature Name	Release Information	Feature Description
Default Enablement of SD-AVC	Cisco Catalyst SD-WAN Control Components Release 20.18.1	The Cisco SD-AVC component is enabled by default in new Cisco Catalyst SD-WAN environments. The control for enabling or disabling is in **Administration** > **Settings** > **SD-AVC**.
Cloud-hosted SD-AVC Service for On-premises Environments	Cisco Catalyst SD-WAN Control Components Release 20.18.1	This release extends the use of a cloud-hosted SD-AVC service to on-premises installations of Cisco Catalyst SD-WAN where internet access is available.

Cisco SD-AVC

Default enablement

From SD-WAN Control Components 20.18.1, the SD-AVC component is enabled by default in new Cisco Catalyst SD-WAN installations. The enablement applies to all Cisco SD-WAN Manager nodes.

Upgrade from releases earlier than SD-WAN Control Components 20.18.1

For Cisco Catalyst SD-WAN environments that have been upgraded from releases earlier than SD-WAN Control Components 20.18.1, SD-AVC is not necessarily enabled. The status of SD-AVC enablement before

upgrade is preserved after upgrade. The control for enabling or disabling is in **Administration** > **Settings** > **SD-AVC**.

Cloud-hosted SD-AVC service

From Cisco Catalyst SD-WAN Control Components Release 20.10.1, some Cisco Catalyst SD-WAN environments have used a cloud-hosted SD-AVC service instead of a local service. Specifically, these installation types have used cloud-hosted SD-AVC:

- Cisco Cloud-delivered Catalyst SD-WAN
- Cisco Hosted Catalyst SD-WAN

Cisco Catalyst SD-WAN Control Components Release 20.18.1 extends the use of the cloud-hosted SD-AVC service to on-premises installations of Cisco Catalyst SD-WAN where internet access is available, and where Cloud Services are enabled. In air-gapped environments without internet access, or if the Cloud Services feature is not enabled, Cisco Catalyst SD-WAN uses a local SD-AVC service.

Benefits of the cloud-hosted SD-AVC service

- Resources

  Using the cloud-hosted SD-AVC service reduces the load on SD-WAN Manager host resources.

- Service maintenance

  Cisco can provide patches to the cloud-hosted SD-AVC service at any time, optimizing SD-AVC operation.

Supported solutions for the cloud-hosted SD-AVC service

SD-WAN

Restrictions for the cloud-hosted SD-AVC service

- Compliance for government installations

  For compliance reasons, some government installations of Cisco Catalyst SD-WAN do not use all available cloud services, including cloud-hosted SD-AVC.

- Upgrade information

  This information is relevant only if you have upgraded your Cisco Catalyst SD-WAN environment from a release earlier than Cisco Catalyst SD-WAN Control Components Release 20.18.1.

Upgraded from	Conditions	Result
Release earlier than Cisco Catalyst SD-WAN Control Components Release 20.18.1	Cloud services and SD-AVC enabled	The upgraded environment uses the cloud-hosted SD-AVC service.
	Either Cloud Services disabled, or SD-AVC disabled	The upgraded environment uses the local SD-AVC service. After upgrading, if you enable Cloud Services (**Administration** > **Settings** > **Cloud Services**), the environment switches to using the cloud-hosted SD-AVC service.

Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later

Installing or upgrading to Cisco vManage Release 20.3.1 automatically includes installation of Cisco SD-AVC as a component.

For information about Cisco SD-AVC, see Cisco SD-AVC, on page 25.

Enable Cisco SD-AVC, Cisco vManage Release 20.3.1 through SD-WAN Manager 20.16.x

Enabled by default

From SD-WAN Manager 20.18.1, SD-AVC is enabled by default.

Prerequisites

Ensure that routers in the network that are included in the Cisco Catalyst SD-WAN topology have a DNS server configured.

Note Cisco SD-AVC must operate on only one Cisco SD-WAN Manager instance. In a Cisco SD-WAN Manager cluster, enable Cisco SD-AVC on only one instance of Cisco SD-WAN Manager.

To enable Cisco SD-AVC, perform the following steps.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
2. For the desired host (the portal on which you are enabling SD-AVC), click **...** and select **Edit**.
3. In the **Edit Manager** pop-up window, select the checkbox for **Enable SD-AVC**.

Note The **Edit Manager** pop-up window provides an option for disabling the application server. After disabling the application server, you cannot later enable other services using this method. If you need to disable the application server, do not do this at the same time that you enable other features.

4. Enter the username and password, using Cisco SD-WAN Manager credentials. Reboot the device to apply the changes.
5. After the reboot, Cisco SD-WAN Manager comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.
6. (optional) After installation is complete, you can verify that Cisco SD-WAN Manager has the SD-AVC virtual service installed and operating correctly.
   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
   b. Click **Service Configuration**, in the Cisco SD-WAN Manager row of the table. Verify that SD-AVC indicates that it is reachable.

Enable SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices

To enable SD-AVC on the Cisco IOS XE Catalyst SD-WAN device, create a localized policy that enables **app visibility** and apply the policy to the template for the Cisco IOS XE Catalyst SD-WAN device.

Prerequisites

- A template exists for the Cisco IOS XE Catalyst SD-WAN device (example: Cisco ASR 1001-X, Cisco ISR 4321).
- TCP port 10501 destination traffic must be permitted.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
   a. Click **Add Policy**.
   b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
   c. In the **Policy Overview** screen, enter a policy name and policy description.
   d. Select **Application**.
   e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. For the device on which you have to enable SD-AVC, click **…** and select **Edit** from the menu.
   c. Click **Additional Templates**.
   d. Add the localized policy created in an earlier step of this procedure.
   e. Click **Update** and proceed through the next screens to push the updated template to the device.

5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.

```
show avc sd-service info summary
```

or

```
show avc sd-service info connectivity
```

Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier



Note Beginning with Cisco vManage Release 20.3.1/Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the Cisco SD-AVC installation has changed. See Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later, on page 79.

Overview

Beginning with the 18.4 release, Cisco Catalyst SD-WAN can optionally incorporate Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco IOS XE Catalyst SD-WAN devices. The SD-AVC network service operates as a container within Cisco SD-WAN Manager.

What are the benefits of this feature?

Cisco SD-AVC uses Cisco NBAR2 and other components that operate on devices in the network to provide:

- Recognition of network application traffic for visibility, analytics, application-aware routing, and application-based policies, such as QoS and application-based firewall policy.
- Analytics at the network level.

Cisco SD-AVC Installation Requirements for Cisco SD-WAN Manager

The following table describes the SD-AVC installation requirements.

Cisco SD-WAN Manager Installation Scenario	Requirements
Cisco vManage 18.4 on a cloud-based server, provided fully configured by the Cisco cloud operations team	The SD-AVC package is pre-installed by the Cisco cloud operations team.
Cisco vManage 18.4 on a self-managed cloud or local server	Install the SD-AVC package as described below.
Upgrading from an earlier version of Cisco SD-WAN Manager to Cisco vManage 18.4	Install the SD-AVC package as described below.

Enabling SD-AVC on Cisco SD-WAN Manager

Prerequisites

- Download the latest container image for the SD-AVC network service. Save the file to an accessible location on the server hosting Cisco SD-WAN Manager. This container is required for the procedure. To download the container, open the Cisco Software Download page and enter "SD-WAN". Select "Software-Defined WAN (SD-WAN)" from the results, then "SD-WAN" in the results. In the software packages available for download, select SD-AVC.
- Ensure that routers in the network that are included in the SD-WAN topology have a DNS server configured.
- The virtual machine in which Cisco SD-WAN Manager operates must have the following resources available to dedicate to the SD-AVC network service:
  - vCPU: 4
  - RAM: 5 GB
  - Storage: 40 GB

Procedure

1. Ensure that the downloaded SD-WAN image is compatible with your version of Cisco SD-WAN Manager.
   a. Display the checksum for the compatible image, using the following API:

      https://*[vManage-IP-address]*/dataservice/sdavc/checksum

      Example: https://10.0.0.1/dataservice/sdavc/checksum

   b. Verify that the checksum of the downloaded image matches this.
2. To upload the SD-AVC virtual service package to Cisco SD-WAN Manager:
   a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
   b. Click **Virtual Images** and select **Upload Virtual Image** to upload the SD-AVC package.
3. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** page.
4. For the desired host (the Cisco SD-WAN Manager portal on which you are enabling SD-AVC), click **…** and choose **Edit**.
5. In the Edit Cisco SD-WAN Manager dialog box, enter the username and password, using Cisco SD-WAN Manager credentials.
6. Select the checkbox for **Enable SD-AVC**. Click **Update**.
7. Cisco SD-WAN Manager prompts you to confirm before rebooting the device to apply the changes to the device. Click **OK** to confirm.
8. After the reboot, Cisco SD-WAN Manager comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.

9. (Optional) After installation is complete, you can verify that Cisco SD-WAN Manager has the SD-AVC virtual service installed and operating correctly.
   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
   b. In Service Configuration, in Cisco SD-WAN Manager row of the table, verify that the SD-AVC shows a green checkmark.

For information about Cisco SD-WAN Manager commands, see *Cisco SD-WAN Manager Command Reference* documentation.

Enable SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices

To enable SD-AVC on the Cisco IOS XE Catalyst SD-WAN device, create a localized policy that enables **app visibility** and apply the policy to the template for the Cisco IOS XE Catalyst SD-WAN device.

Prerequisites

- A template exists for the Cisco IOS XE Catalyst SD-WAN device (example: Cisco ASR 1001-X, Cisco ISR 4321).
- TCP port 10501 destination traffic must be permitted.

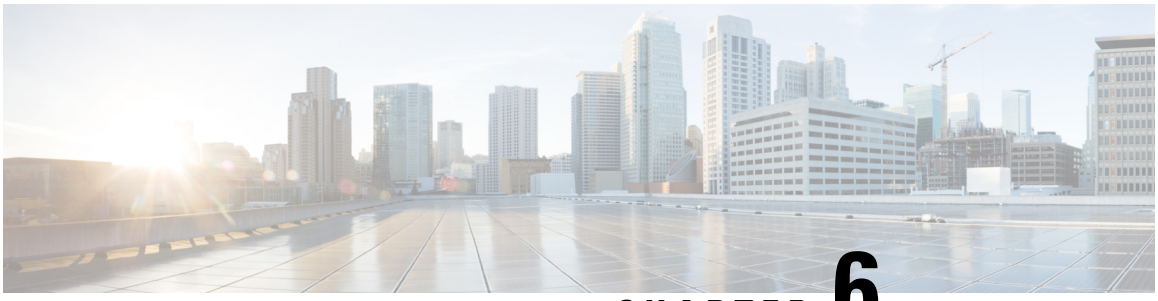
Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
   a. Click **Add Policy**.
   b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
   c. In the **Policy Overview** screen, enter a policy name and policy description.
   d. Select **Application**.
   e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. For the device on which you have to enable SD-AVC, click **…** and select **Edit** from the menu.
   c. Click **Additional Templates**.
   d. Add the localized policy created in an earlier step of this procedure.
   e. Click **Update** and proceed through the next screens to push the updated template to the device.
5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.

```
show avc sd-service info summary
```

or

```
show avc sd-service info connectivity
```



CHAPTER 6

Cisco SD-AVC Cloud Connector

- Cisco SD-AVC Cloud Connector feature history, on page 85
- Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later, on page 86
- Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x, on page 87
- Enable Cloud Services, on page 92

Cisco SD-AVC Cloud Connector feature history

Table 8: Feature History

Feature Name	Release Information	Description
Cisco SD-AVC Cloud Connector	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	When enabling Cloud onRamp for SaaS to manage Office 365 traffic, you can limit best path selection to apply only to some Office 365 traffic, according to the Office 365 traffic categories defined by Microsoft, or to include all Office 365 traffic. The Cisco SD-AVC Cloud Connector provides support for this functionality.
Update to the SD-AVC Cloud Connector Enablement	Cisco vManage Release 20.10.1	Beginning with this release, enabling the Cloud Connector requires a cloud gateway URL and a one-time password (OTP) instead of a client ID and client secret.
New Procedure for Enabling Cisco SD-AVC Cloud Connector	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Control Components Release 20.14.1	This release introduces a new procedure for enabling Cisco SD-AVC Cloud Connector from the Cloud Services option in **Administration** > **Settings**. From this release, enabling Cloud Connector does not require an OTP or opening a TAC case.

Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later

Before Cisco Catalyst SD-WAN Manager Release 20.14.1, client ID, client secret credentials, and sometimes a cloud gateway URL and OTP were required to enable Cloud Connector. From Cisco Catalyst SD-WAN Manager Release 20.14.1, you can configure Cisco SD-AVC Cloud Connector using the Cloud Services page. With this feature, you need not retrieve an OTP or create a TAC case separately to enable SD-AVC Cloud Connector.

Prerequisites

Enable Cisco SD-AVC under **Administration** > **Cluster Management** to enable Cloud Connector.

Enable Cisco SD-AVC Cloud Connector Using Cloud Services

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Cloud Services**.
3. Enable **Cloud Services** in the **Cloud Services** tab.

   From Cisco Catalyst SD-WAN Manager Release 20.18.2, after you enable Cloud Services, click **Register** in the **Cisco services onboarding popup** that appears and enter your Smart Account credentials.

   Alternatively, from Cisco Catalyst SD-WAN Manager Release 20.18.2, you can authenticate for Cloud Services from the **Cisco services registration** page.
4. Enter your Smart Account credentials.
5. (Optional) Enable **Analytics**.



Note Enable this option only if you have deployed Cisco Catalyst SD-WAN Analytics, and have confirmed that it is reachable by Cisco SD-WAN Manager.

6. Enable **SD-AVC Cloud Connector**.



Note If Cisco SD-WAN Manager is cloud-hosted by Cisco, this option does not appear and Cloud Connector is enabled automatically after you enable the Cloud Services option.

7. Click **Save**.

Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x

Before You Begin

- Before Cisco vManage Release 20.10.1, enabling Cloud Connector required client ID and client secret credentials. From Cisco vManage Release 20.10.1, it requires a cloud gateway URL and OTP. An advantage to using an OTP is that, in contrast to a client secret, it does not expire. See the following table for details about the credentials required for different releases, upgrade scenarios, and hosting options.
- Cisco SD-AVC Cloud Connector is a necessary component for Cloud onRamp for SaaS to manage Office 365 traffic according to the Office 365 traffic category.

Table 9: Requirements to Enable SD-AVC Cloud Connector

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
Cisco vManage Release 20.3.1 to Cisco vManage Release 20.9.x	All hosting options	**Required credentials**: Client ID Client secret (As explained in the procedure, open the Cisco API Console page to create Cloud Connector credentials if you do not already have credentials.) **Note** When you receive a message in Cisco SD-WAN Manager indicating that SD-AVC credentials are expiring, return to the Cisco API Console and create new Cloud Connector credentials. **Other requirements**: Enable SD-AVC in cluster management, as described here.

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
Upgrade an existing instance to Cisco vManage Release 20.10.1 from an earlier release	All hosting options	**Notes**: In this scenario, the SD-AVC components operate differently than in earlier releases. Consequently, running the **request nms all status** command on the Cisco SD-WAN Manager instance shows that the "NMS SDAVC server" component is not enabled. This is expected behavior, and does not indicate any problem with SD-AVC. Note that the "NMS SDAVC gateway" component shows as enabled.
	Cisco-hosted	**Required credentials**: • Cloud gateway URL: Use: https://datamanagement-us01.sdwan.cisco.com/validate_sdavc/ • OTP: Use the Cisco Catalyst SD-WAN Portal to get the OTP. See the Cisco Catalyst SD-WAN Portal Configuration Guide for details. **Other requirements**: Enable SD-AVC in cluster management, as described here.
	Self-managed, hosted in a public cloud, a private cloud, or on-premises	

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
		Required credentials: • If Cloud Connector was already enabled at the time of the upgrade, the client ID and client secret credentials continue to work until the client secret expires. When the client secret expires, an alarm appears in Cisco SD-WAN Manager to indicate the expiration. At this point, enabling Cloud Connector requires the cloud gateway URL and OTP. Use datamanagement-us-01.sdwan.cisco.com for the URL, and open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. • If Cloud Connector was not enabled at the time of the upgrade, enabling Cloud Connector requires the cloud gateway URL and OTP. Use datamanagement-us-01.sdwan.cisco.com for the URL, and open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. **Other requirements**: Before enabling the Cloud Connector, enable SD-AVC in cluster management, as described here.

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
Fresh installation of Cisco vManage Release 20.10.1 and later	Cisco-hosted	**Required credentials**: Cloud Connector is enabled by default, without requiring manual entry of credentials. You can use the Cisco Catalyst SD-WAN Portal to view the OTP if needed. See the Cisco Catalyst SD-WAN Portal Configuration Guide for details. **Other requirements**: Enable SD-AVC in cluster management, as described here. **Notes**: In this scenario, the SD-AVC components operate differently than in earlier releases. Consequently, running the **request nms all status** command on the Cisco SD-WAN Manager instance shows that the "NMS SDAVC server" component is not enabled. This is expected behavior, and does not indicate any problem with SD-AVC. Note that the "NMS SDAVC gateway" component shows as enabled.
	Self-managed, hosted in a public cloud, a private cloud, or on-premises	**Required credentials**: • Cloud gateway URL: Use https://datamanagement-us01.sdwan.cisco.com/validate_sdavc/ • OTP: Open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. **Other requirements**: Enable SD-AVC in cluster management, as described here.

Enable Cisco SD-AVC Cloud Connector

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

2. Click **SD-AVC** and enable **Cloud Connector**.

   (If you are using Cisco vManage Release 20.10.x, Cisco vManage Release 20.11.x, or Cisco Catalyst SD-WAN Manager Release 20.12.x, click **Edit** and enable **Cloud Connector**.)

   (In Cisco vManage Release 20.9.x and earlier releases, the option is called **SD-AVC Cloud Connector**. In these releases, click **Edit** and enable **Cloud Connector**.)



Note If Cisco SD-WAN Manager is cloud-hosted by Cisco, this option does not appear and Cloud Connector is enabled automatically.

3. (This step applies to Cisco vManage Release 20.10.1 and later, and is handled automatically if Cisco SD-WAN Manager is Cisco-hosted.)

   See the **Before You Begin** section that precedes these steps for details about the requirements for enabling the SD-AVC Cloud Connector in different scenarios. As noted there, enable SD-AVC in cluster management before enabling the Cloud Connector.

   If you need to enter the cloud gateway URL, use: datamanagement-us-01.sdwan.cisco.com

   If you need to use the Cisco Catalyst SD-WAN Portal to get the OTP, see the Cisco Catalyst SD-WAN Portal Configuration Guide for details.

   If you need to open a TAC case to receive the OTP, open https://mycase.cloudapps.cisco.com/case. The workflow for receiving the OTP requires the following:

   - Entitlement information.
   - Smart Account.
   - Virtual Account.
   - The organization name configured in Cisco SD-WAN Manager.
   - Cisco SD-WAN Manager geographic location: Americas, European Union (EU), or Asia-Pacific (APAC).
   - Technology: Use Cisco Catalyst SD-WAN On-Prem for an on-prem installation or Cisco Catalyst SD-WAN - Cisco-Hosted for a Cisco-hosted installation.
   - SubTechnology: Use SDWAN Cloud Infra.

4. (For Cisco vManage Release 20.9.x and earlier releases) Enter the following credentials:

   - Client ID



Note Click (**i**) for **Client ID** and open the Cisco API Console page in a browser window to create Cloud Connector credentials if you do not already have credentials.

   - Client Secret
   - Organization Name: Use the descriptive name that you entered on the Cisco API Console page in the **Name of your application** field.

5. (Releases earlier than Cisco vManage Release 20.10.1) For **Affinity**, you can select a geographical location for storing the Cloud Connector data. For organizations located in Europe, it is recommended to change the location to Europe, in accordance with EU General Data Protection Regulation (GDPR) regulations.
6. For **Telemetry**, you can optionally disable the collection of telemetry data.

Note If Cisco SD-WAN Manager is cloud-hosted by Cisco, this option does not appear and telemetry is enabled automatically.

Create Credentials on the Cisco API Console

The following steps show how to create credentials in the Cisco API Console. These steps are provided here for convenience, and are subject to change.

1. On the Cisco API Console page, sign in using your Cisco credentials.
2. Click **My Apps and keys**. A page opens for registering a new application.
3. To register SD-AVC, follow the steps below:
   a. Name of your application: Use any descriptive name. Save this name for a later step.
   b. In the **Application Type** area, click Service.
   c. In the **Grant Type** area, check the **Client Credentials** check box.
   d. Check the **Hello API** check box.
   e. In the **Terms of Service** section, check the check box to agree with the terms.
   f. Click **Register**. The Cisco API Console page displays the Client ID and Client Secret details. Keep this page open to complete the procedure.

Note When you receive a message in Cisco SD-WAN Manager indicating that SD-AVC credentials are expiring, return to the Cisco API Console and create new Cloud Connector credentials.

Enable Cloud Services

While a Protocol Pack upgrade for devices in the network is in process, or is scheduled and pending, you cannot enable Cloud Services.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Cloud Services**.

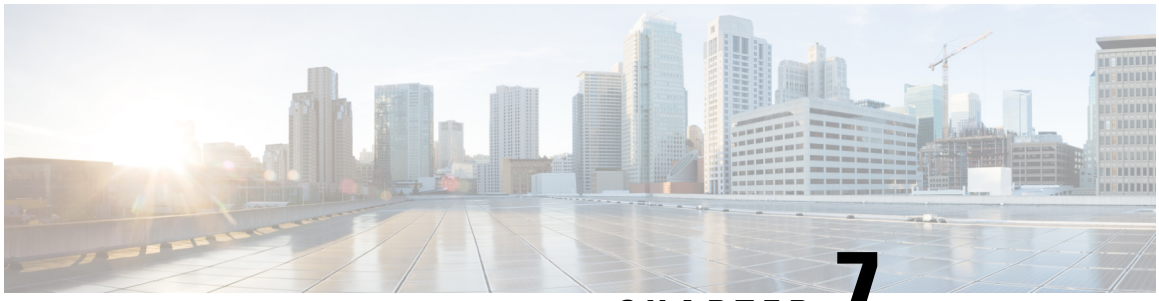
Step 3 Enable **Cloud Services** in the **Cloud Services** tab.

Step 4 Enter your Smart Account credentials in the fields.

Step 5 (Optional) Enable **Analytics**.

Note
Enable this option only if you have deployed Cisco SD-WAN Analytics, and have confirmed that it is reachable by Cisco SD-WAN Manager.

Step 6 Click **Save**.



CHAPTER 7

Install and Upgrade for Cisco Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later

- Install and Upgrade Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later, on page 96
- Platforms Supported in Controller Mode, on page 96
- Cisco IOS XE Image Compatibility, on page 97
- Upgrade Considerations, on page 98
- Restrictions, on page 99
- Self-Signed Trustpoint, on page 100
- Introducing Autonomous and Controller Mode, on page 100
- Software Installation for Cisco IOS XE Routers, on page 101
- Plug and Play in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later Releases, on page 103
- Non-PnP Onboarding, on page 106
- Mode Discovery and Mode Change with Bootstrap Files, on page 109
- Reset Controller Mode Configuration, on page 111
- Mode Switching: Additional Information, on page 113
- Verify Controller and Autonomous Modes, on page 113
- Change the Console Port Access After Installation, in Controller Mode, on page 114
- Upgrade to Cisco IOS XE Release 17.2.1r or Later, on page 116
- Downgrade from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or Later Releases, on page 120
- Restore Smart Licensing and Smart License Reservation, on page 122
- Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing, on page 122
- Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices, on page 124
- Troubleshooting, on page 125

Install and Upgrade Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later

Table 10: Feature History

Feature Name	Release Information	Description
Install and Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature supports the use of a single "universalk9" image to deploy Cisco IOS XE Catalyst SD-WAN and Cisco IOS XE functionality on all the supported devices. This universalk9 image supports two modes - Autonomous mode (for Cisco IOS XE features) and Controller mode (for Cisco Catalyst SD-WAN features) .
Cisco Catalyst 8000V Edge SoftwarePlatform	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Support added for the Cisco Catalyst 8000V Edge Software platform. Upgrading Cisco CSR1000V or Cisco ISRv platforms to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a includes upgrading to the platform type to the Cisco Catalyst 8000V.

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, use the universalk9 image to deploy both Cisco IOS XE Catalyst SD-WAN and Cisco IOS XE on Cisco IOS XE Catalyst SD-WAN devices.

Starting Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, UCMK9 image is not available.

This release helps in seamless upgrades of both the Cisco Catalyst SD-WAN and non Cisco Catalyst SD-WAN features and deployments.

Access the Cisco IOS XE and Cisco IOS XE Catalyst SD-WAN functionality through Autonomous and Controller execution modes, respectively. The Autonomous mode is the default mode for the routers and includes the Cisco IOS XE functionality. To access Cisco IOS XE Catalyst SD-WAN functionality, switch to the Controller mode. You can use the existing Plug and Play Workflow to determine the mode of the device.

Platforms Supported in Controller Mode

Platforms Supported in Controller Mode

- Cisco ASR 1000 Series Aggregation Services Routers
- Modular Cisco ASR 1006-X with ASR1000-RP3 module (Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later, see Cisco ASR 1006-X with an RP3 Module.)

- Cisco ISR 1000 Series Integrated Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco 1101 Industrial Integrated Services Router
- Cisco CSR 1000v Series Cloud Services Routers
- Cisco Integrated Services Virtual Router (ISRv)
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms
- Cisco Catalyst 8000V Edge Software (Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or later)

Platforms Not Supported in Controller Mode

Modular platforms based on the following ASR 1000 Series Routers are not supported in controller mode:

- ASR1000-RP2

Crypto Modules Supported in Controller Mode

The following crypto modules are required for the ASR 1000 series routers:

- ASR1001HX-IPSECHW, for the ASR 1001-HX
- ASR1002HX-IPSECHW, for the ASR 1002-HX

Cisco IOS XE Image Compatibility

Deployment Image Version	Cisco Catalyst SD-WAN	Non Cisco Catalyst SD-WAN
Cisco IOS XE Releases 16.9.x, 16.10.x, 16.11.x, 16.12.x	ucmk9	universalk9
Cisco IOS XE Release 17.1.x	NA	universalk9
Cisco IOS XE Release 17.2.x and later	universalk9*	universalk9**

- * For Cisco Catalyst SD-WAN use case, non-LI and non-payload encryption image types are not supported.
- ** For non Cisco Catalyst SD-WAN use case, non-LI and non-payload encryption image types are supported (universalk9_noli, universalk9_npe, universalk9_npe_noli).

Upgrade Considerations

The following Cisco IOS XE Catalyst SD-WAN devices support multirate interfaces and support the 1GE small form-factor pluggable (SFP) (optical and CU) and 10GE SFP+ (optical and CU) modules on their 10G interfaces ports:

- Cisco ASR 1001-HX Router
- Cisco Catalyst 8500-12X4QC
- Cisco Catalyst 8500-12X

These devices support auto-negotiation on 10G interfaces ports with 1GE SFP (optical and CU) modules. The following notes apply to auto-negotiation in both SD-WAN and non-SD-WAN modes of the above three router models only:

- For releases before Cisco IOS XE 17.6.1a, auto-negotiation can be configured using the CLI.
- For releases before Cisco IOS XE 17.6.1a, if you use the CLI or Cisco Catalyst SD-WAN to reboot a device with a 10G interface that includes a 10GE SFP+ module, that interface will not come up. In this situation, use Cisco Catalyst SD-WAN or the CLI to configure **`no negotiation auto`** for the interface, then reboot the device.
- From Cisco IOS XE Release 17.6.3a, **`auto neg`** values for auto-negotiation are pushed to 10G interfaces on supported devices through feature templates. Ensure that you know which SFP module is on which 10G interface on a device so that you can properly configure the feature template.
- On software releases upto Cisco IOS XE Release 17.6.3a, the **`negotiation auto`** command is not supported on a 10G interface that includes a 10GE SFP+ module.
- From Cisco IOS XE Release 17.6.4 onwards, the negotiation auto command is supported on a 10G interface with 10 GE SFP+ module. In this scenario, in the output of **`show interface Tengig x/x/x`**, the link type is force-up regardless of **`negotiation auto/no negotiation auto`** configuration. The same is applicable when the configurations are pushed through Cisco SD-WAN Manager template.
- From Cisco IOS XE Release 17.6.4 onwards, the negotiation auto command is supported on a 10G interface that includes a 1GE Fiber and Copper SFP.
- On software releases upto Cisco IOS XE Release 17.6.3a, the **`no negotiation auto`** command with the default OFF option must be sent through a feature template to all 10G interfaces that include a 10GE SFP+ module. Otherwise, the template push fails.
- Before upgrading to Cisco IOS XE Release 17.6.3a, use a feature template, a CLI add-on feature templates, or the CLI to **`apply no negotiation auto`** to all 10G interfaces that include a 10GE SFP+ module.
- If you upgrade to Cisco IOS XE Release 17.6.3a from a release in which auto-negotiation was enabled on a 10G interface that includes a 10GE SFP+ module, that interface will not come up. In this situation, use the CLI to configure **`no negotiation auto`** for the interface after the upgrade completes.
- Before upgrading to Cisco Catalyst SD-WAN Manager Release 20.12.1 or Cisco IOS XE Catalyst SD-WAN Release 17.12.1a or later releases, contact Cisco TAC to check and drop any non-compatible indexes. Non-compatible old index can impact successful upgrade to newer version.

- In ASR 1001-HX, multi-rate supported only on last 4 ports of bay1 8X10G/1G.
- After upgrading the device, configurations for new features in the updated version are not applied automatically. To enable these new features, you must manually redeploy the template or configuration group.

Following notes are applicable for C8300, C8500L-8S4X models of routers:

- From Cisco IOS XE Release 17.15.1 onwards, the **negotiation auto** command is supported on a 10G interface that includes a 10GE SFP+ module.
- From Cisco IOS XE Release 17.15.1 onwards, on a 10G interface that includes a 10GE SFP+ module, in the output of **show interface Tengig x/x/x** the link type will show as force-up always regardless of **negotiation auto/no negotiation auto** configuration. The same is applicable when the configurations are pushed through Cisco SD-WAN Manager template.
- The command **show running config** does not display **no neg auto** for dual rate ports in controller mode. Where as **show sdwan running-config** shows **no neg auto**. In case of **neg auto** configuration, the command **show interfaces <interface num>** always display for dual rate ports with 10G optics.

Table 11: Auto Negotiation Configurations

C8500			
SFPs	Default Auto Negotiation	Default Speed	Default Duplex
1G Copper	OFF	1000M	Full
1G Optical	OFF	1000M	Full
10G Optical	OFF	10000M	Full
C8300			
1G Copper	ON	1000M	Full
1G Optical	ON	1000M	Full
10G Optical	ON	10000M	Full

Note Ensure that negotiation configuration matches with the peer device interface settings. If there is a mismatch in the interface settings, the interface may go down.

Restrictions

Restrictions for single "universalk9" image

- Dual-IOSd is supported only in autonomous mode.

- Images without payload encryption and NO-LI (universalk9_npe, universalk9_noli, universalk9_npe_noli) images are not supported in controller mode. Only universalk9 images are supported.
- After onboarding and determining the mode of operation, changing from Controller mode to Autonomous mode or vice-versa, results in the loss of configuration.
- Reset button functionality is not supported in controller mode on Cisco ISR 1000 series Integrated Service Routers. The reset button does not function to restore a golden image or configuration in controller mode.
- Auto-install (Python and TCL scripts) and ZTP—Autoinstall and ZTP are not supported in controller mode. If DHCP discovers an attempt to install using either of these processes, a mode change to Autonomous mode is triggered.
- WebUI—In controller mode, WebUI is not supported and an error message is displayed, if used.

Self-Signed Trustpoint

A self-signed trustpoint is generated and loaded to a Cisco IOS XE Catalyst SD-WAN device when the device boots up. If this trustpoint is deleted for any reason, you can generate and load a new trustpoint by rebooting the device. The new key may be different than the deleted one.

Introducing Autonomous and Controller Mode

The Cisco IOS XE Catalyst SD-WAN Release 17.2.1r release introduces two installation modes – Autonomous and Controller modes. The autonomous mode supports the functionality of Cisco IOS XE non Cisco Catalyst SD-WAN deployment and the controller mode supports the Cisco Catalyst SD-WAN solution.

The following are the main differences between Autonomous mode and Controller mode:

Table 12:

Feature	Autonomous Mode	Controller Mode
Configuration Method	• Command Line Interface (CLI) • NETCONF	YANG-based configuration • Cisco SD-WAN Manager • NETCONF
Onboarding Modes	• Plug and Play • Config-Wizard • WebUI • Bootstrap (USB, bootflash, and so on) • Auto-Install (Python Script, TCL Script) • ZTP (Using DHCP Option 150 and Option 67)	• Plug and Play • Bootstrap (USB, bootflash, and so on)

Feature	Autonomous Mode	Controller Mode
Licensing	Cisco Smart Licensing	Cisco High Performance Security (HSEC) software licensing. No device licensing.
Image Type	Universalk9	Universalk9
Dual-IOSd redundancy model	Supported	Not Supported
High Availability	Supported	Not Supported
Global configuration mode	configure terminal	config-transaction

Software Installation for Cisco IOS XE Routers

Download the Software for Cisco IOS XE Release 17.2.1r or Later

Download the *router-model*-universalk9.*release-number*. image for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later software from the Cisco site https://software.cisco.com .

Install Software on Cisco ASR, Cisco ISR and Cisco ENCS Platforms

Refer to the following documents for installation instructions:

- Cisco ISR 1000 Series Integrated Services Router
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Installing Cisco Enterprise NFVIS on Cisco ENCS 5100 and ENCS 5400

Install Software on Cisco CSR 1000v Platform

Based on the cloud in which you are deploying the CSR 1000v instance, see the following to perform the bootstrap and/or the day 0 configuration:

- Deploying the OVA to the VM
- Manually creating the Cisco CSR 1000v VM using the .iso file (Citrix XenServer)
- Creating a CSR 1000v VM using the self installing .run package
- Manually creating the VM using the .iso file (Microsoft Hyper-V)
- Booting the CSR 1000v Instance
- Deploying a CSR 1000v VM Using Custom Data
- Deploying a CSR 1000v VM on Microsoft Azure

Install a Cisco Catalyst 8000V Edge Software Platform

Table 13: Feature History

Feature Name	Release Information	Description
Support for the Cisco Catalyst 8000V Edge Software Platform on OpenStack Train	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This feature introduces support for managing a Cisco Catalyst 8000V Edge software platform hosted in the OpenStack cloud computing platform "Train" release.

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco Catalyst SD-WAN supports the Cisco Catalyst 8000V virtual router platform, which replaces the Cisco CSR1000V and Cisco ISRv. Installing the Cisco Catalyst 8000V in an Cisco Catalyst SD-WAN environment requires Cisco vManage Release 20.4.1 or later.

Download the Cisco Catalyst 8000V software image that is appropriate for your method of deployment. For example, this can be an OVA file for ESXi, or a QCOW2 image for OpenStack or KVM. Do not choose an ISO image. Have the image ready to upload to the Cisco SD-WAN Manager software image repository. The file name begins with: c8000v-universalk9

Note To operate with Cisco Catalyst SD-WAN, the device must be in controller mode. When starting the device in controller mode, boot the device using the bootflash:packages.conf file.

For complete information about the platform, including installation in KVM, ESXi, and OpenStack environments, see the Cisco Catalyst 8000V Edge Software Installation and Configuration Guide. For information about creating a bootstrap file for onboarding the Cisco Catalyst 8000V into Cisco Catalyst SD-WAN, see Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices.

Clean Install

We recommend a clean install of the Cisco Catalyst 8000V. This ensures support for all features, provides the most up-to-date licensing, and ensures that devices and the controller stay synchronized. For cases where upgrade is necessary, see the procedure in **Upgrade to Cisco IOS XE Release 17.2.1r or Later**.

Note After a clean install of the Cisco Catalyst 8000V, it is not possible to downgrade the device to a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.4.1a.

Upgrading a Cisco CSR1000V to a Cisco Catalyst 8000V

Upgrading a Cisco CSR1000V or Cisco ISRv virtual router to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a includes upgrading to the Cisco Catalyst 8000V. Note the following:

- The Cisco Catalyst 8000V preserves all of the functionality available on Cisco CSR1000V or Cisco ISRv platforms.

- Performing the upgrade in Cisco SD-WAN Manager preserves the configuration of the device(s) being upgraded.

OpenStack

Installing a Cisco Catalyst 8000V on the OpenStack Train release requires using a Cisco IOS XE Catalyst SD-WAN Release 17.7.1a or later image for the Cisco Catalyst 8000V.

Cisco does not support installing a Cisco Catalyst 8000V on OpenStack using an earlier image, or installing on OpenStack using an earlier image and upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

Plug and Play in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later Releases

Plug and Play Onboarding Workflow

1. Place an order for the device in Cisco Commerce with Smart Account and Virtual Account details of the customer.
2. The device information from Cisco Commerce like Device serial number, Smart Account, and Virtual Account are added to the Plug and Play portal.
3. Add a Cisco SD-WAN Validator controller profile into the Plug and Play (PnP) portal for the same Smart Account and Virtual Accounts.
4. Associate the new device to the Cisco SD-WAN Validator controller profile manually.
5. PnP sends all relevant information including Cisco SD-WAN Validator details, device serial number, organization name, and network ID to Zero Touch Provisioning (ZTP).
6. Download the device serial number file (provisioning file) from PnP and upload it to Cisco SD-WAN Manager. The devices are now available on Cisco SD-WAN Manager. You can also use the **Sync Smart Account**option on Cisco SD-WAN Manager to sync the device with your virtual account and populate the device in Cisco SD-WAN Manager.

Note If you created and scheduled a device template on Cisco vManage Release 20.3.x and upgraded Cisco SD-WAN Manager to Cisco vManage Release 20.4.1 or later before onboarding the target device, when you onboard the device using PNP or ZTP, the template push fails. To avoid this failure, reschedule the template after upgrading the Cisco SD-WAN Manager software and then onboard the device.

Note If the ZTP process for a device is interrupted because the device reloads or power cycles, the ZTP process does not restart and the device comes online with the Cisco SD-WAN Manager image that was in its original configuration. In this situation, upgrade the device to the desired Cisco SD-WAN Manager release manually.

Note For more information, refer to the Plug and Play Support Guide.

Mode Discovery with Plug and Play Onboarding

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change, if required. The mode change results in a reboot of the device. Once reboot is complete, the device performs appropriate discovery process.

When you upgrade to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, on a Cisco device that already runs a Cisco IOS XE or Cisco Catalyst SD-WAN image, the device starts in autonomous mode or controller mode depending on the configured controller.

Plug and Play (PnP) deployment include the following discovery process scenarios:

Table 14:

Boot up Mode	Deployment Mode	On-boarding agent	Cisco SD-WAN Validator	Discovery Process	Mode Change
Autonomous	Cisco Digital Network Architecture (DNA)	Plug and Play	No	Plug and Play Connect Discovery or on-premise plug and play server discovery	No Mode change
Autonomous	Cisco SD-WAN Manager	Plug and Play	Yes	Plug and Play Connect Discovery	Mode change to controller mode
Controller	Cisco DNA	Plug and Play	No	Plug and Play Connect Discovery or on-premise plug and play server discovery	Mode change to autonomous mode
Controller	Cisco SD-WAN Manager	Plug and Play	Yes	Plug and Play Connect Discovery	No mode change

Automatic IP Address Detection

Table 15: Feature History

Feature Name	Release Information	Description
Day 0 WAN Interface Automatic IP Detection using ARP	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enables a device to automatically learn about the available IP addresses and default gateway information when a DHCP server is not available. The device assigns an IP address to its WAN interface, and then contacts the PnP server and begins the PnP onboarding process.

Typically, the WAN interface on a Cisco IOS XE Catalyst SD-WAN device or Cisco vEdge device is configured as a DHCP client, and this interface receives an IP address and gateway server information from the DHCP server during the plug-and-play (PnP) onboarding process.

If the DHCP server is not available, the device automatically learns about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets. If an IP address that the device learns allows a successful connection to the PnP server, the device continues with the PnP onboarding process.

Note This feature applies only to day zero deployments and is enabled by default.

Prerequisites for Automatic IP Address Detection

- To trigger ARP, configure the IP address of the device as the BGP neighbor on the provider edge (PE) router.

  This PE router is the first point of contact for the device in the WAN transport network. The PE router then sends ARP packets with this IP address to the device. The device receives the ARP packets, and then the Automatic IP Address Detection feature defines the ARP destination IP address as the device's WAN interface IP address.

- For Cisco IOS XE Catalyst SD-WAN devices, the network mask of this IP address must be 30 bits.
- For automatic IP address detection and redirection through an on-premises ZTP server, the A record of the ZTP server on the DNS server must be set to ztp.cisco.com. In addition, the DNS server must have an ip name-server value of 8.8.8.8 or 8.8.4.4.

For automatic IP address detection, a device uses 8.8.8.8 or 8.8.4.4 as the DNS server to resolve devicehelper.cisco.com or ztp.cisco.com. The PnP process then attempts to reach devicehelper.cisco.com or ztp.cisco.com to continue onboarding.

Note An IP address that a device automatically detects is not preserved during reboots of the device that occur before the PnP onboarding completes. In such cases, an IP address is assigned automatically when the PE router ARP cache expires.

Limitations and Restrictions for Automatic IP Address Detection

The following limitations and restrictions apply only to Cisco IOS XE Catalyst SD-WAN devices:

- This feature is supported only on Cisco 1000 Series Integrated Service Routers, Cisco 4000 Series Integrated Service Router, and Cisco Catalyst 8200 and 8300 Series Edge Platforms. On these devices, this features is supported only for Gigabit Ethernet Interface 0/0/0.
- The feature is supported only on devices that are in controller (SD-WAN configuration) mode. See https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/install-upgrade-17-2-later.html.
- This feature is supported only in a simple 30 bit network mask Layer 2 network in which one PE router and one customer edge router are in the same VLAN.
- This feature does not support VRRP, HSRP, or GLBP on the PE router.
- An ARP destination IP address is used as the WAN interface IP address on a device only after the device receives the same ARP request eight times within an interval of 150 seconds.

Non-PnP Onboarding

Creating a Cisco Catalyst SD-WAN Bootstrap Configuration File

See On-Site Bootstrap Process for Cisco Catalyst SD-WAN Devices and Generate a Bootstrap File For Cisco IOS XE Catalyst SD-WAN Devices Using the CLI for information about generating a bootstrap file.

New Installation: Mode Change Device Day Zero Scenario

1. If the device is running a pre-17.2 universalk9 image on a new box, or for an existing box where you performed **write erase** and **reload** and loaded a Cisco IOS XE 17.2 or newer image, the device boots in day zero configuration and in autonomous mode.
2. The new device determines if a mode change is required based on the bootstrap file.
   - If ciscosdwan.cfg or ciscosdwan_cloud_init.cfg bootstrap file in a plugged in the bootstrap location, mode change to controller mode is initiated. After the device boots up in controller mode, the configuration present in the configuration file is applied.
   - If a ciscortr.cfg bootstrap file or config-wizard is discovered, mode change is not initiated and the boot up continues in the Autonomous mode.

Note

- The bootstrap file (ciscosdwan.cfg) is generated by Cisco SD-WAN Manager, and has UUID, but no OTP.
- For software devices (Cisco Catalyst 8000V Edge Software, Cisco Cloud Services Router 1000V Series, and Cisco ISRv), and for OTP-authenticated devices such as the Cisco ASR1002-X, use the bootstrap file ciscosdwan_cloud_init.cfg. This file has OTP but no UUID validation.

Switch Modes Using Cisco CLI

Use the **controller-mode** command in privileged EXEC mode to switch between controller and autonomous modes.

Autonomous Mode

The **controller-mode reset** command takes the device back to day zero configuration.

```
Device# controller-mode reset
```

The **controller-mode disable** command switches the device to autonomous mode.

```
Device# controller-mode disable
```

Note **controller-mode disable** should only be used for temporarily operating the device in autonomous mode. Ensure the device is returned to controller mode using the same image.

Controller Mode

Note To switch the device to the controller-mode, boot the system using either the bootflash:/*.bin or bootflash:/packages.conf file.

Note If bootflash:core or harddisk:core contain core files (files containing information about process crashes), move the files to another location before changing the device to controller mode. If these files remain in the bootflash:core or harddisk:core directories, Cisco SD-WAN Manager displays an alarm after onboarding the device. You can move the files to any other directory on the device other than a core directory.

The **controller-mode enable** command switches the device to controller mode.

```
Device# controller-mode enable
```

Notes

Note	Description
Bundle mode	If device is booted with bundle mode (Super packages), after reboot, the image gets automatically expanded and activated to prepare the router for SDWAN operation. Devices with 4GB RAM may require an additional reboot to free up space in /bootflash. The following devices with 4GB RAM need reload: • Cisco ISR 4451 • Cisco ISR 4431 • Cisco ISR 4461 • Cisco ISR 4351 • Cisco ISR 4331 • Cisco ISR 4321
Viewing the contents of the bootflash:/.sdwaninstaller directory	You cannot view the contents of the bootflash:/.sdwaninstaller directory of a Cisco IOS XE Catalyst SD-WAN device in either of the following conditions: • The device is in controller mode. or • The device is in autonomous mode and using Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later.

Change a device to Controller mode

Changing from Autonomous mode to Controller mode requires the device to perform an operation that expands the software package of the current running image. The expand operation requires bootflash space. When you execute the **controller-mode enable** command to change to Controller mode, there is a possibility that the router does not have enough bootflash space to expand the software package of the running image. The first step of the procedure addresses this.

Procedure

Step 1 Check the available space on the device bootflash. Ensure that there is space equal to the size of the software image .bin file plus 100 MB.

Step 2 Use the **controller-mode enable** command on the device to change to Controller mode.

The device verifies that the bootflash has sufficient space to expand the software image file.

If there is sufficient bootflash space, the device reboots in Controller mode and expands the software image.

If the bootflash does not have sufficient space, the command output indicates the space required and the device does not change to Controller mode.

Note
The device verifies that the bootflash has sufficient space to expand the software image file, from these releases:

- Cisco IOS XE Catalyst SD-WAN Release 17.12.5a and later maintenance releases of 17.12.x
- Cisco IOS XE Catalyst SD-WAN Release 17.15.2 and later maintenance releases of 17.12.x
- Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and all later releases

In earlier releases, the **controller-mode enable** command does not first verify that the bootflash has sufficient space to expand the software image file. It first changes the device to Controller mode, then expands the file. To verify that the device expanded the image file and to troubleshoot if it did not, see Troubleshoot software image expansion failure due to lack of bootflash space.

Mode Discovery and Mode Change with Bootstrap Files



Note If your Cisco IOS XE Catalyst SD-WAN device is already running an older Cisco Catalyst SD-WAN configuration version or file and when you upgrade your device from Cisco IOS XE Catalyst SD-WAN Release 16.x to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, the device boots up in the controller mode. To prevent the device from booting up in the controller mode, before performing the device upgrade, ensure that you remove the stale Cisco Catalyst SD-WAN configuration file from the bootflash.

Detailed steps to delete all Cisco Catalyst SD-WAN artifacts from bootflash:

delete /force bootflash:/ciscosdwan*.cfg

delete /force /recursive bootflash:/.sdwaninstallerfs

delete /force /recursive bootflash:/.sdwaninstaller

delete /force /recursive bootflash:/.sdwaninternal

delete /force /recursive bootflash:/sdwan

delete /force /recursive bootflash:/vmanage-admin

delete /force /recursive bootflash:/.cdb_backup

delete /force /recursive bootflash:/.installer/active

delete /force /recursive bootflash:/.installer

On a device that already runs a Cisco Catalyst SD-WAN image, after upgrading to a Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later image, the device boots up in controller mode.



Note Installing the Cisco Catalyst 8000V on OpenStack requires using the Cisco Catalyst 8000V image for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a or later.

Use the **controller-mode enable** command to switch from autonomous to controller mode and the **controller-mode disable** command to switch from controller mode to autonomous mode.

To switch modes using CLI, ensure that the appropriate configuration files mentioned in the table below are present. After the device boots up, the configuration present in the configuration file is applied. The device reads the configuration file and uses the configuration information to come up on the network.

Table 16: Configuration File Prerequisites for Mode Change

Current Mode	Mode change to	Platforms	Configuration file and location
Controller	Autonomous	All supported platforms	ciscortr.cfg in any file system available to the device
Autonomous	Controller	• Cisco Cloud Services Router, CSR1000v • Cisco Integrated Services Virtual Router, ISRv • Cisco Catalyst 8000V • Cisco ASR1002-X	ciscosdwan_cloud_init.cfg on bootflash, USB, CDROM0, or CDROM1
Autonomous	Controller	• Cisco Aggregation Services Router, ASR 1000 Series • Cisco Integration Service Routers, ISR 4000 series and ISR 1000 series routers	ciscosdwan.cfg on bootflash or USB

Note On a Cisco CSR1000v device (for Cisco IOS XE Release 17.2 or later) and a Cisco Catalyst 8000V (for Cisco IOS XE Release 17.4 or later) image deployment, if you want to boot up the device in controller mode, load the bootstrap file generated by Cisco SD-WAN Manager by bootstrap (ESXi, KVM, and OpenStack) or user-data (AWS) or custom-data (Azure and GCP).

The following fields must be present in the ciscosdwan_cloud_init.cfg bootstrap file:

- otp
- uuid
- vbond
- org

Note When the device mode is switched from autonomous to controller, the startup configuration and the information in NVRAM (certificates), are erased. This action is equivalent to running the **write erase** command.

Note When the device mode is switched from controller to autonomous, all Yang-based configuration is preserved and can be reused if you switch back to controller mode.

Note When the device is in Day N configuration and is reloaded, the presence of a bootstrap file does not impact the device operating mode.

Note You cannot view the contents of the bootflash:/.sdwaninstaller directory and .sdwanistallerfs file of a Cisco IOS XE Catalyst SD-WAN device in either of the following conditions:

- The device is in controller mode.

  or

- The device is in autonomous mode and using Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later.

Directory, more, copy and delete operations are not allowed when the file and directory are hidden in controller-mode.

Reset Controller Mode Configuration

If you use **request platform software sdwan config reset** or **request platform software sdwan software reset** commands to bring the device back to controller-mode day-zero configuration, the device performs one of the following actions:

- Performs mode discovery. For more information on mode discovery, see Mode Discovery with Plug and Play Onboarding, on page 104.
- Uses the appropriate configuration file to perform bootstrap. For more information on the Cisco Catalyst SD-WAN bootstrap configuration file, see Creating a Cisco Catalyst SD-WAN Bootstrap Configuration File, on page 106.

To erase the Cisco Catalyst SD-WAN configuration of the current active image, use the following CLI:

```
Device# request platform software sdwan config reset
%WARNING: Bootstrap file doesn't exist and absence of it can cause loss of connectivity to
 the controller.
For saving bootstrap config, use:
request platform software sdwan bootstrap-config save
Proceed to reset anyway? [confirm]
Backup of running config is saved under /bootflash/sdwan/backup.cfg
WARNING: Reload is required for config-reset to become effective.
```

Note The warning listed in the above configuration is visible only on Cisco IOS XE Catalyst SD-WAN Release 17.3.1a and later images.

For the changes to take effect, you must reload the router after running the CLI. Running this CLI ensures the configuration for the currently installed version is wiped along with crypto keys and the device enters the day zero workflow after the reload.

If the device is not set up to use PnP for onboarding, then it reads the configuration file in the bootflash and uses the configuration information to come up on the network. If the device is setup to use PnP onboarding, then after reload, the PnP discovery will start again.

Note In the case of public clouds, just like a fresh install, additional bootstrap configuration is provisioned that allows you to login to the instance.

Note In public cloud and NFVIS environments, ensure that a latest day-zero bootstrap configuration file (exported from Cisco SD-WAN Manager) is available in a supported location and following standard file naming conventions (example: bootflash:/ciscosdwan_cloud_init.cfg file), before the configuration reset operation is performed.

Warning Failure to follow save the bootstrap file in these environments cause loss of virtual machine connectivity.

Configuration Reset

When you do a configuration reset, the device performs the following:

- Erases only the configuration of the current running image.
- Erases the certificates.
- Reboots the router with the same image. At this point, the device repeats Day-0 boot up.

Software Reset

When you do a software reset, the device performs the following:

- Erases all SD-WAN metadata saved in the `bootflash:/sdwan` folder including certificates.
- Erases configuration of all the images (running as well as previously activated).
- Removes all image files except the one marked as default.
- Reboots the router with the default version image. At this point, the device repeats Day-0 boot up.

Mode Switching: Additional Information

Configuration Persistence During Mode Switch

Table 17:

Current Configuration Mode	Mode Switched to	Behavior
Autonomous	Controller	Contents of NVRAM and the startup configuration are erased. Configuration is not be restored. Device is reverted to Day zero configuration. Previous running configuration is stored in bootflash. **Note** When you switch from autonomous mode to controller mode, and switch back to autonomous mode, the Cisco IOS XE configuration is not restored because the startup configuration is empty. You have to manually restore configuration from the backup.
Controller	Autonomous	CDB contents are erased (for subsequent mode switches) and Cisco IOS configuration are not restored (as startup configuration is empty). You have to manually restore configuration from the backup.

Verify Controller and Autonomous Modes

Show Command Output for Controller Mode

```
Device# show logging | include OPMODE_LOG
*Dec  8 16:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in CONTROLLER mode

Device# show version | inc operating

Router operating mode: Controller-Managed

Device# show platform software device-mode
Operating device-mode: Controller

Device-mode bootup status:
------------------------------------
 Success

Device# show platform software chasfs r0 brief | inc device_managed_mode

/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [controller]
  /tmp/fp/chasfs/etc/device_managed_mode : [controller]

Device# show version | inc Last reload
Last reload reason: Enabling controller-mode
```

Show Command Output for Autonomous Mode

```
Device# show logging | include OPMODE_LOG
*Dec  8 17:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Device# show version | inc operating

Router operating mode: Autonomous

Device# show platform software device-mode

Operating device-mode: Autonomous

Device-mode bootup status:
------------------------------------

Device# show platform software chasfs r0 brief | inc device_managed_mode

/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [autonomous]
  /tmp/fp/chasfs/etc/device_managed_mode : [autonomous]

Device# show version | inc Last reload
Last reload reason: Enabling autonomous-mode
```

Note If the device is in controller mode, the **show sdwan running-config** command does not display the following information:

- All service commands under /native/service except tcp-small-servers, udp-small-servers, tcp-keepalives-in, and tcp-keepalives-out
- Configurations under line VTY except for transport, access-class, and ipv6 access-class
- IPv6 unicast routing configuration
- Commands in /native/enable

To verify these configuration use the **show running-config** command.

Change the Console Port Access After Installation, in Controller Mode

Before You Begin

Before beginning this procedure, ensure that you have access to the Cisco CSR1000V or Cisco Catalyst 8000V router through the currently configured console access method.

Change the Console Port Access

This procedure changes the method for connecting to the console to access a Cisco CSR1000V or Cisco Catalyst 8000V software device.

The image used for deploying the Cisco CSR1000V or Cisco Catalyst 8000V software determines the default type of console access to use, which can be virtual or serial.

The procedure includes changing the mode from controller to autonomous, and then back to controller, which is required for operation with Cisco Catalyst SD-WAN. These mode changes cause the device to reload.

Perform the following steps to change the console port access.

1. In EXEC mode, enter **enable** to enter privileged EXEC mode.

   ```
   Router> enable
   ```

2. Disable controller mode. Enter the following command and follow the prompts to complete the command.

   ```
   Device# controller-mode disable
   ```

Note This reboots the device in autonomous mode.

3. After the device restarts, enter **enable** to enter privileged EXEC mode.

   ```
   Router> enable
   ```

4. Enter global configuration mode.

   ```
   Device# configure terminal
   ```

5. Use one of the following options to configure the type of access:

   - virtual: This option specifies that the device is accessed through the hypervisor virtual VGA console.

     ```
     Device(config)# platform console virtual
     ```

   - serial: This option specifies that the device is accessed through the serial port on the virtual machine (VM).

Note

- Use this option only if your hypervisor supports serial port console access.
- If the device configuration is stored as a Cisco SD-WAN Manager device template and is attached to the device using Cisco SD-WAN Manager, enter the command

  ```
  Device(config)# platform console serial
  ```

  to the CLI add-on feature template. For more information on CLI Add-On Feature Templates see, Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide. This helps in avoiding Cisco SD-WAN Manager removing the serial port when the device template is attached to the device.

```
Device(config)# platform console serial
```

   - auto: (This option has been deprecated and is not recommended.) This option specifies that the device console is detected automatically. This is the default setting during the initial installation boot process. For additional information, see Booting the Cisco CSR 1000v as the VM.

6. Exit configuration mode.

   ```
   Device(config)# end
   ```

7. Save the configuration.

```
Device# write memory
```

8. Copy the running configuration to the startup configuration.

```
Device# copy system:running-config nvram:startup-config
```

9. Change the device back to controller mode. Enter the following command and follow the prompts to complete the command.

```
Device# controller-mode enable
```

Note This step reboots the device in controller mode.

Upgrade to Cisco IOS XE Release 17.2.1r or Later

Supported Upgrades

Table 18: Cisco CSR1000V and Cisco ISRv Routers

You Can Upgrade to...	From these Releases
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Cisco IOS XE SD-WAN 17.3.1a or later Cisco IOS XE SD-WAN 17.2.2 or later Cisco IOS XE SD-WAN 16.12.4a or later **Note** • To upgrade a Cisco CSR1000V or Cisco ISRv router to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from a release not listed here requires first upgrading to one of these releases. • Upgrading a Cisco CSR1000V or Cisco ISRv router to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a includes upgrading to the Cisco Catalyst 8000V.
Cisco IOS XE 17.3.x	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco IOS XE Release 17.2.1v Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

You Can Upgrade to...	From these Releases
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

Table 19: All Routers Supported by Cisco Catalyst SD-WAN Except Cisco CSR1000V, Cisco ISRv, and Cisco Catalyst 8000V

You Can Upgrade to...	From these Releases
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Cisco IOS XE SD-WAN 17.3.1a or later Cisco IOS XE SD-WAN 17.2.1 or later Cisco IOS XE SD-WAN 16.12.4a or later
Cisco IOS XE 17.3.x	
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

Use the following procedures to upgrade your device to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later images.

Note Do not delete the existing image to ensure that you have a rollback option.

Note If an upgrade fails, do not attempt to reactivate the new software image. Instead, remove the new software image, identify and correct any configuration settings that might have caused the failure, and try the upgrade procedure again. If the issue persists, contact Cisco for assistance.

Note When upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from Cisco IOS XE Releases 17.3.1a or earlier, we recommend that you do not make any changes to the device configuration using CLI, while a feature template is detached. Starting Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, we use Cisco Catalyst SD-WAN assisted upgrades. In this upgrade procedure, Cisco Catalyst SD-WAN saves the device configuration before the upgrade. If the configuration on the device, that is modified using CLI is not same as on Cisco Catalyst SD-WAN, then the device has inconsistent configuration after the upgrade.

For example, if you configure the BGP AS number of a device to a different value using CLI, the device can have inconsistent configuration and the upgrade fails. If the upgrade is performed when the device is in CLI mode, then you must revert the BGP AS number to the original value and then upgrade the device. Therefore, we recommend that you upgrade the device using Cisco Catalyst SD-WAN.

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, if you are upgrading the firmware for a device on which the primary tunnel interface is a cellular interface and the backup tunnel interface is a gigabit interface, use the gigabit interface as the primary interface for the firmware upgrade.

For information about configuring the priority of a tunnel interface, see the vmanage-connection-preference command in *Cisco Catalyst SD-WAN Command Reference*. An interface that is configured with a higher preference value has a higher priority.

Upgrade Using Cisco Catalyst SD-WAN

We recommend using Cisco SD-WAN Manager to upgrade. This keeps devices and the controller synchronized.

1. Use the Cisco SD-WAN Manager upgrade and activate procedure described in the *Cisco Catalyst SD-WAN Monitor and Maintain* guide.

Upgrade Using CLI

We recommend using Cisco SD-WAN Manager to upgrade. This keeps devices and the controller synchronized. If it is necessary to upgrade using the CLI, use the following steps.

Back Up Configuration Files

Use these following steps to make configuration file copies before performing the manual upgrade process. Without these steps, the router will lose its configuration during the upgrade.

Note If the deployment is on a public cloud service, such as Amazon Web Services (AWS), failure to save the configuration before upgrading manually can cause an unrecoverable loss of connectivity with the device. In contrast to a hardware device, there may be no way to gain any type of console access to the virtual router.

1. Use the following command to make a backup copy of the Cisco IOS XE Catalyst SD-WAN configuration:

```
show running-config | redirect bootflash:/sdwan/ios.cli
```

2. Use the following command to make a backup copy of the Cisco Catalyst SD-WAN running configuration:

```
show sdwan running-config | redirect bootflash:/sdwan/sdwan.cli
```

Upgrade Procedure

1. Download the Cisco IOS XE Release 17.2 image for your device from https://software.cisco.com
2. Upload the image to the device.
3. Install the new software. Example:

   ```
   Device# request platform software sdwan software install
   bootflash:/isr4300-universalk9.17.2.1.SPA.bin
   ```

4. Activate the software. The device reloads when the activation is complete. Example:

   ```
   Device# request platform software sdwan software activate 17.2.01r.9.3
   ```

5. Verify that the software is activated.

   ```
   Device# show sdwan software

   VERSION      ACTIVE DEFAULT PREVIOUS CONFIRMED TIMESTAMP
   ------------------------------------------------------------------------------
   16.12.1d.0.48 false  true   true     auto     2020-03-04T10:43:45-00:00
   17.2.01r.9.3   true  false  false    user     2020-03-04T11:15:20-00:00

   Total Space:388M Used Space:100M Available Space:285M
   ```

6. (Optional) To ensure that the new version is preserved if software reset required, use the following command. Example:

   ```
   Device# request platform software sdwan software set-default 17.2.01r.9.3
   ```

7. Verify the upgrade using **request platform software sdwan software upgrade-confirm**.

   ```
   Device# request platform software sdwan software upgrade-confirm
   ```

Note From 17.6.1 release, you cannot perform another install, activate or deactivate operation for an image or a Software Maintenance Update (SMU), when the upgrade-confirm function is pending for an existing operation.

Note In controller mode, use the **config-transaction** command to enter global configuration mode. The **configuration terminal** command is not supported in Controller mode.

Table 20: Configuration Persistence in Upgrade Scenarios

Existing Installation (image)	Upgraded to (image)	Behavior
Cisco IOS XE SD-WAN Release 16.12 and earlier (ucmk9)	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r (universalk9)	Device boots up in controller mode and configuration is preserved.

Existing Installation (image)	Upgraded to (image)	Behavior
Cisco IOS XE Release 16.12 and earlier (universalk9)	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r (universalk9)	Device boots up in autonomous mode and configuration is preserved (via startup configuration).

Downgrade from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or Later Releases

Downgrade a Cisco IOS XE Catalyst SD-WAN Device to a Previously Installed Software Image

To downgrade a Cisco IOS XE Catalyst SD-WAN device to an earlier software image that is currently installed on the device using the CLI, perform the following steps:

1. Display the currently installed images.

   ```
   Device# show sdwan software
   ```

   ```
   Example:
   VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
   ------------------------------------------------------------------------------
   16.10.400.0.0    false   true     true      auto       2019-11-20T04:40:05-00:00
   17.3.1.0.102822  true    false    false     auto       2020-07-31T11:01:22-00:00
   ```

2. Activate the image. This resets the device, deleting any existing configuration. The device starts in day zero configuration.

   ```
   Device# request platform software software activate desired-build
   ```

   Example:

   ```
   Device# request platform software software activate 16.10.400.0.0
   ```

Downgrade a Cisco IOS XE Catalyst SD-WAN Device to an Older Software Image

To download an earlier software image and downgrade a Cisco IOS XE Catalyst SD-WAN device to an earlier software image using the CLI, perform the following steps:

1. Display the currently installed images.

   ```
   Device# show sdwan software
   ```

   ```
   Example:
   VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
   ------------------------------------------------------------------------------
   16.10.400.0.0    false   true     true      auto       2019-11-20T04:40:05-00:00
   17.3.1.0.102822  true    false    false     auto       2020-07-31T11:01:22-00:00
   ```

2. If necessary, remove an existing software image to provide space for loading a new software image.

```
Device# request platform software sdwan software remove previous-installed-build
```

Example:

```
Device# request platform software sdwan software remove 16.10.400.0.0
```

3. Download the software image for the downgrade and copy it to the device bootflash.
4. Install the downloaded image.

```
Device# request platform software sdwan software install bootflash:/desired-build
```

Example:

```
Device# request platform software sdwan software install
bootflash:/isr1100be-universalk9.17.02.01a.SPA.bin
```

5. Display the currently installed images, which now include the new image.

```
Device# show sdwan software
VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
17.02.01a.0.211  false    true     true      auto       2020-03-30T09:34:04-00:00
```

6. Activate the new image. This resets the device, deleting any existing configuration. The device starts in day zero configuration.

```
Device# request platform software sdwan software activate desired-build clean
```

Example:

```
Device# request platform software sdwan software 17.02.01a.0.211 clean
```

Downgrade Scenarios for Cisco IOS XE Release 17.2.x

Table 21: Configuration Persistence in Downgrade Scenarios

Existing Installation (image)	Downgrade to (image)	Behavior
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r(universalk9) in controller mode	Cisco IOS XE SD-WAN Release 16.12 and earlier (ucmk9)	Device boots up with ucmk9 image and configuration is restored if the uckm9 image was previously installed on the device. Downgrading to a fresh install of old image versions brings the device to Day 0 configuration. To proceed, use the **clean** option at activation.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r (universalk9) in autonomous mode	Cisco IOS XE Release 17.1.1 and earlier (universalk9)	Device boots up with universalk9 image and configuration is restored.

Note

- Downgrading directly from controller mode to Cisco IOS XE Amsterdam Release 17.1.x or earlier universalk9 or other non Cisco Catalyst SD-WAN images is not supported. To downgrade from controller mode to earlier IOS XE images, switch to autonomous mode and follow the downgrade process.
- Downgrading directly from autonomous mode to Cisco IOS XE SD-WAN 16.12 or earlier ucmk9 SD-WAN images is not supported. To downgrade from autonomous mode to earlier Cisco IOS XE Catalyst SD-WAN images, switch to controller mode and follow the downgrade process.

Restore Smart Licensing and Smart License Reservation

The smart licensing authorization is lost when a device switches from autonomous to controller mode and back to autonomous mode again.

For more information about Smart Licensing, refer to Smart Licensing Guide for Access and Edge Routers.

Restore Smart Licensing

1. Reconfigure device to reach Cisco Smart Software Manager (CSSM).
2. Register the device using **license smart register idtoken** *token* **force** command in privileged EXEC mode.
3. Set the required crypto throughput using **platform hardware throughput crypto** *crypto-value*.
4. Save the configuration using **write memory** in privileged EXEC mode.
5. Reload the device and verify that the new crypto throughput value is applied using the **show platform hardware throughput crypto** command.

Restore Smart License Reservation

1. Enable the reservation mode using the **license smart reservation** command in global configuration mode.
2. Set the required crypto throughput using **platform hardware throughput crypto** *crypto-value*.
3. Save the configuration using **write memory**.
4. Reload the device and verify that the new crypto throughput value is applied using the **show platform hardware throughput crypto** command.

Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing

To onboard a Cisco Catalyst 8000V platform hosted by a cloud service, using pay as you go (PAYG) licensing, perform these steps.

You can also use Cisco Cloud onRamp for Multi-Cloud to onboard a Cisco Catalyst 8000V platform using PAYG licensing. For information to integrate public cloud infrastructure into the Cisco Catalyst SD-WAN fabric, see Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x.



Note This procedure is applicable to Cisco Catalyst 8000V hosted by Amazon Web Services (AWS).

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, and click **Add PAYG WAN Edges**.
2. In the **Add PAYG WAN Edges** dialog box, enter the number of PAYG devices to onboard into Cisco Catalyst SD-WAN, select the **Validate** check box, and click **Add**.

   The **Task View** page opens, showing the progress as Cisco SD-WAN Manager creates logical devices.



Note Validating causes Cisco SD-WAN Manager to publish the list of devices to the Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller controllers in the network.

3. After the **Task View** page shows the logical devices have been created successfully, choose **Configuration** > **Devices** to view the new logical devices on the **Devices** page.



Note The **Chassis Number** column shows the unique identifier for each logical device.

4. For the logical devices that you have created, click **…** and choose **Generate Bootstrap Configuration**.
5. (Optional) Attach a device template to the logical devices that you have created.
6. In the **Generate Bootstrap Configuration** dialog box, click **Cloud-Init** and then click **OK**.

   The **Generate Bootstrap Configuration** dialog box shows the content of the bootstrap configuration, which includes the UUID of the logical device, and includes the configuration details provided by the device template if you have attached one.



Note The UUID corresponds to the identifier in the **Chassis Number** column in the **Devices** table.

7. There are different methods for loading the bootstrap configuration onto a C8000V instance on a cloud service. The method you use depends on the cloud service. We recommend to click **Download** in the **Generate Bootstrap Configuration** dialog box to save a copy of the bootstrap configuration.
8. In the cloud services portal, create a PAYG instance of the Cisco Catalyst 8000V. When configuring the instance, use the bootstrap configuration that you created in Cisco SD-WAN Manager. The details of how to load the Cisco Catalyst SD-WAN bootstrap configuration onto the instance are specific to the cloud services provider.

Note On AWS, the workflow for bringing up an instance includes a user data step that enables loading the bootstrap configuration.

9. On the cloud service platform, start the Cisco Catalyst 8000V instance using the bootstrap configuration from an earlier step.

   When the Cisco Catalyst 8000V instance boots up, it joins the Cisco Catalyst SD-WAN overlay automatically. In Cisco SD-WAN Manager, on the **Devices** page, this Cisco Catalyst 8000V instance shows a green medal icon in the **State** column and **In Sync** in the **Device Status** column.

Note On the **Devices** page, for logical devices that have not joined the Cisco Catalyst SD-WAN overlay, the **State** column shows a dotted-circle icon.

Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices

Before You Begin

The device template provides the configuration details that enable the device to connect to Cisco SD-WAN Manager.

If you create a logical device and then generate a bootstrap configuration without first attaching a device template, the resulting file will include a minimal configuration. If you attach a device template to the logical device before generating the bootstrap configuration, the resulting file will include a more complete configuration, which can be helpful in enabling the device to connect to the Cisco Catalyst SD-WAN overlay. We recommend that you attach a device template to the logical device before creating the bootstrap configuration.

This procedure is useful when onboarding a software device, such as the Cisco Catalyst 8000V, to a private cloud, such as KVM, ESXi, or OpenStack.

Bootstrap Process for Cisco SD-WAN Cloud-Hosted Devices

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. For the logical device (includes the UUID) that you are using for a new cloud-hosted instance, click **…** and choose **Generate Bootstrap Configuration**.
3. In the **Generate Bootstrap Configuration** dialog box, choose **Cloud-Init** and click **OK**. The **Generate Bootstrap Configuration** dialog box displays the bootstrap configuration, including the OTP token for the license, Cisco SD-WAN Validator address, UUID, and organization information.

Note The UUID corresponds to the identifier in the **Chassis Number** column in the **Devices** table.

Note Ensure that the bootstrap configuration does not include more interfaces than the virtual device instance has in the cloud environment.

4. There are different methods for loading the bootstrap configuration onto a device instance on a cloud service. The method you use depends on the cloud service. We recommend that you click **Download** in the **Generate Bootstrap Configuration** dialog box to save a copy of the bootstrap configuration.

   You can use the bootstrap configuration when setting up a device instance in the cloud service. The configuration enables the device instance to connect to Cisco Catalyst SD-WAN.

For information about onboarding a Cisco Catalyst 8000V in a private cloud, see the following:

- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide, Installing in KVM Environments
- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide, Installing in VMware ESXi Environment
- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide, Installing in OpenStack

Troubleshooting

Troubleshooting Software Installation

Router Loads the Previous Software Version After Booting

Router Loads the Previous Software Version After Booting

Problem

A router starts up using the previously installed software version.

Conditions

A router using Cisco IOS XE has two or more software versions installed.

Possible Causes

If the router begins booting up, and power cycles during the bootup, it may reboot using the previously installed software version.

Note Cisco IOS XE devices have a mechanism that preserves the previously installed software version. As a safeguard against getting stuck during bootup with a corrupted software image, a device can fall back to the previously installed software version. This fallback can also occur if the device experiences a power cycle during bootup. In this case (power cycle during bootup), you can reboot the device to load the latest software.

Solutions

1. Check the active and inactive system software versions for a device using one of the following procedures:
   - Cisco SD-WAN Manager procedure:
     a. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
     b. Click a device name in the **Hostname** column.
     c. In the left pane, click **Real Time**.
     d. In the **Device Options** field, enter **Software Versions**.

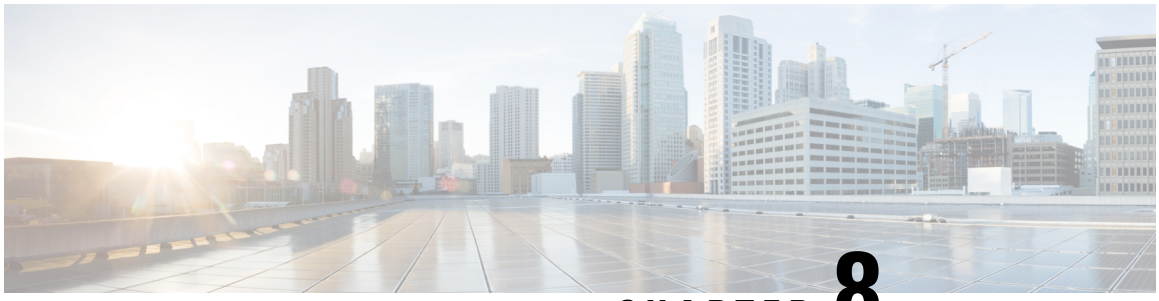
        A table displays the installed software versions and indicates which version is active.

   - CLI procedure:
     a. Execute the **show sdwan software** command in privileged EXEC mode to view the current active software version and the previous version.
     b. Execute the **show version** command on the device, in privileged EXEC mode.

        If the device is using the latest installed software version, the command output shows bootflash:packages.conf.

        If the device is using the previous software version, the command output shows bootflash:prev_packages.conf.

2. Reboot the device and check the loaded system software again.
3. If the device boots again with the previous software version (bootflash:prev_packages.conf), contact Cisco TAC for assistance.



CHAPTER 8

Cisco Catalyst SD-WAN Overlay Network Bring-Up Process

- Network Overlay Bringup , on page 127
- Cisco SD-WAN Manager Persona and Storage Device, on page 128
- Bring-Up Sequence of Events, on page 129
- Download Software, on page 159
- Deploy Cisco SD-WAN Manager, on page 160
- Deploy Cisco Catalyst SD-WAN Validator, on page 170
- vContainer Host, on page 186
- Deploy Cisco Catalyst SD-WAN Controller, on page 186
- Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals, on page 199
- Deploy Cisco CSR 1000v Using Cloud Service Provider Portals, on page 199
- Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud, on page 200
- Deploy the vEdge Cloud routers, on page 201

Network Overlay Bringup

Table 22: Feature History

Feature Name	Release Information	Description
Disk Encryption in On-Premises ESXi for a Virtual Machine Hosting Cisco SD-WAN Control Components	Cisco Catalyst SD-WAN Control Components Release 20.14.1	With this feature, you can apply disk encryption on the virtual disk When hosting Cisco SD-WAN Control Components in an on-premises installation, using a VMWare ESXi hypervisor hosted on a Cisco UCS platform.

Cisco SD-WAN Manager Persona and Storage Device

When you deploy Cisco SD-WAN Manager, you are prompted to choose a persona (from Cisco vManage Release 20.6.1) and a storage device for the Cisco SD-WAN Manager server the first time that the server boots up after Cisco SD-WAN Manager is installed.

Cisco SD-WAN Manager Persona

From Cisco vManage Release 20.6.1, each Cisco SD-WAN Manager server has a *persona*. The persona defines which services run on the server and defines the role that the server has in a Cisco SD-WAN Manager cluster. For related information on Cisco SD-WAN Manager persona, see "Cisco SD-WAN Manager Cluster."

The persona that is configured for a Cisco SD-WAN Manager server cannot be changed.

Cisco SD-WAN Manager supports the following personas:

- Compute + Data: Includes all services that are required for Cisco SD-WAN Manager, including services that are used for the application, statistics, configuration, messaging, and coordination. This persona should be used for a standalone node, and for the first node in a Cisco SD-WAN Manager cluster.
- Compute: Includes services that are used for the application, configuration, messaging, and coordination. This persona does not include services that are used for statistics. A node with this persona cannot operate as a standalone node and must be part of a Cisco SD-WAN Manager cluster.
- Data: Includes only services that are used for the application and statistics. A node with this persona cannot operate as a standalone node and must be part of a Cisco SD-WAN Manager cluster.

You are prompted to choose a persona for a Cisco SD-WAN Manager server the first time that the server boots up after Cisco SD-WAN Manager is installed. The prompt appears in the command line as follows:

```
1) COMPUTE_AND_DATA
2) DATA
3) COMPUTE
Select persona for vManage (1, 2 or 3):
```

When you see this prompt, type **1** to choose the Compute + Data persona, **2** to choose the Compute persona, or **3** to choose the Data persona. Then type **y** at the **`Are you sure`** prompt that displays to confirm your choice.

When you determine which persona to configure for a server, be aware that a Cisco SD-WAN Manager cluster supports any of the following deployments of nodes:

- Three Compute+Data nodes
- Three Compute+Data nodes and three Data nodes
- Three Compute nodes and three Data nodes (supported only in an upgrade from an existing deployment)

If you require a different combination of nodes, contact your Cisco representative.

Cisco SD-WAN Manager Storage Device

Each Cisco SD-WAN Manager server has a storage device assigned to it. A storage device is a hard drive that is attached to the Cisco SD-WAN Manager server and that contains the /opt/data partition on which the database and other configuration information is saved.

You are prompted to choose a storage device for a Cisco SD-WAN Manager server the first time that the boots up after Cisco SD-WAN Manager is installed. You also are prompted whether you want to format the storage device.

The storage device assignment prompt appears in the command line as follows:

```
Available storage devices:
```

The prompt is followed by a list of available storage devices, each of which is preceded by a number. Type the number that corresponds to the storage device that you want to use for the server.

After you choose a storage device, you are prompted whether to format it. Type **y** to format the storage device, or type **n** to skip formatting. If you format a storage device, all data on the device is permanently deleted.

Bring-Up Sequence of Events

The bring-up process for edge devices—which includes authenticating and validating all the devices and establishing a functional overlay network—occurs with only minimal user input. From a conceptual point of view, the bring-up process can be divided into two parts, one that requires user input and one that happens automatically:

1. In the first part, you design the network, create virtual machine (VM) instances for cloud routers, and install and boot hardware routers. Then, in Cisco SD-WAN Manager, you add the routers to the network and create configurations for each router. This process is described in the Summary of the User Portion of the Bring-Up Sequence.

2. The second part of the bring-up process occurs automatically, orchestrated by the Cisco Catalyst SD-WAN software. As routers join the overlay network, they validate and authenticate themselves automatically, and they establish secure communication channels between each other. For Cisco SD-WAN Validators and Cisco SD-WAN Controllers, a network administrator must download the necessary authentication-related files from Cisco SD-WAN Manager, and then these Cisco SD-WAN Controllers and Cisco SD-WAN Validators automatically receive their configurations from Cisco SD-WAN Manager. For vEdge Cloud routers, you must generate a certificate signing request (CSR), install the received certificate, and then upload the serial number that is included in the certificate to Cisco SD-WAN Manager. After Cisco hardware routers start, they are authenticated on the network and receive their configurations automatically from Cisco SD-WAN Manager through a process called zero-touch provisioning (ZTP). This process is described in the Automatic Portions of the Bring-Up Sequence.

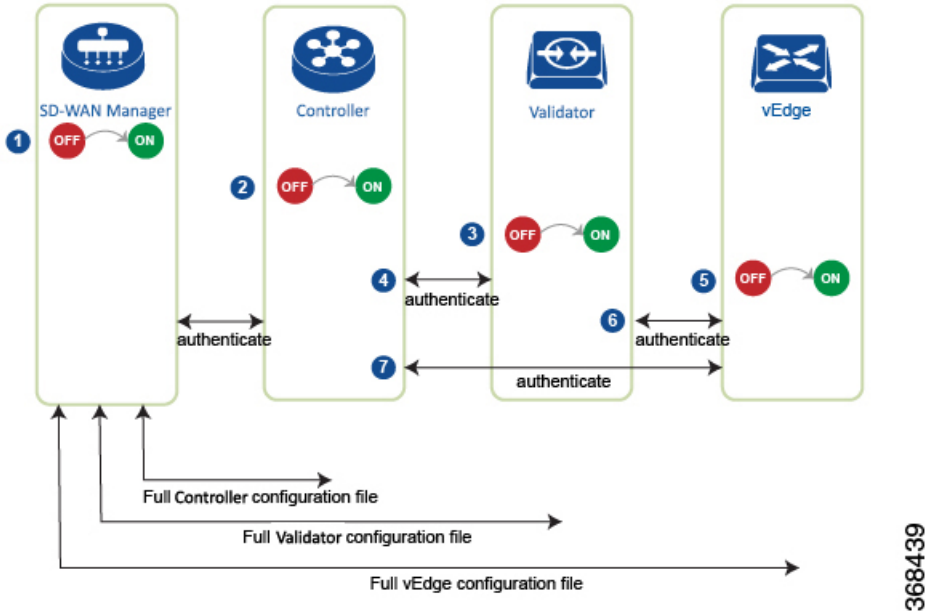
   The end result of this two-part process is an operational overlay network.

   This topic describes the sequence of events that occurs during the bring-up process, starting with the user portion and then explaining how automatic authentication and device validation occur.

Sequence of Events of the Bring-Up Process

From a functional point of view, the task of bringing up the routers in the overlay network occurs in the following sequence:

Figure 10: Bring-Up Sequence of Events



1. The Cisco SD-WAN Manager software starts on a server in the data center.
2. The Cisco SD-WAN Validator starts on a server in the DMZ.
3. The Cisco SD-WAN Controller starts on a server in the data center.
4. Cisco SD-WAN Manager and the Cisco SD-WAN Validator authenticate each other, Cisco SD-WAN Manager and the Cisco SD-WAN Controller authenticate each other, and the Cisco SD-WAN Controller and the Cisco SD-WAN Validator securely authenticate each other.
5. Cisco SD-WAN Manager sends configurations to the Cisco SD-WAN Controller and the Cisco SD-WAN Validator.
6. The routers start in the network.
7. The routers authenticate themselves with the Cisco SD-WAN Validator.
8. The routers authenticate themselves with Cisco SD-WAN Manager.
9. The routers authenticate themselves with the Cisco SD-WAN Controller.
10. Cisco SD-WAN Manager sends configurations to the routers.

Before you start the bring-up process, note the following:

- To provide the highest level of security, only authenticated and authorized routers can access and participation in the Cisco Catalyst SD-WAN overlay network. To this end, the Cisco SD-WAN Controller performs automatic authentication on all the routers before they can send data traffic over the network.
- After the routers are authenticated, data traffic flows, regardless of whether the routers are in a private address space (behind a NAT gateway) or in a public address space.

To bring up the hardware and software components in a Cisco Catalyst SD-WAN overlay network, a transport network (also called a transport cloud), which connects all the routers and other network hardware components, must be available. Typically, these components are in data centers and branch offices. The only purpose of the transport network is to connect all the network devices in the domain. The Cisco Catalyst SD-WAN solution is agnostic with regards to the transport network, and, therefore, can be any type, including the internet, Multiprotocol Label Switching (MPLS), Layer 2 switching, Layer 3 routing, and Long-Term Evolution (LTE), or any mixture of transports.

For hardware routers, you can use the Cisco Catalyst SD-WAN zero-touch provisioning (ZTP) SaaS to bring up the routers. For more information on automatic process to bring-up hardware in the overlay network, see Prepare Routers for ZTP.



Note Starting from Cisco vManage Release 20.3.1, if you assign Cisco SD-WAN Manager VPN0 IP address in the 172.17.0.0/16 subnet, it cannot form control connections to edge devices (IOS XE SD-WAN and SD-routing).

Steps to Bring Up the Overlay Network

Bringing Up the Overlay Network

The following table lists the tasks for bringing up the overlay network using Cisco SD-WAN Manager.

Table 23:

Bring-Up Task	Step-by-Step Procedure
Step 1: Start the Cisco SD-WAN Manager.	**1.** On the hypervisor, create a VM instance. **2.** Boot Cisco SD-WAN Manager server, start the VM, and enter login information. **3.** From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**, configure certificate authorization settings. Select Automated to allow the certificate-generation process to occur automatically when a CSR is generated for a controller device. **4.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**, generate the CSR. **5.** Check for a confirmation email from Symantec that your request has been received. **6.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **7.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, and check if the certificate has been installed.

Bring-Up Task	Step-by-Step Procedure
Step 2: Start the Cisco SD-WAN Validator.	**1.** On the hypervisor, create a VM instance. **2.** Boot the Cisco SD-WAN Validator server and start the VM. **3.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**, add Cisco SD-WAN Validator and generate the CSR. **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. **4.** Check for a confirmation email from Symantec that your request has been received. **5.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **6.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, and check if the certificate has been installed. **7.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for the Cisco SD-WAN Validator. **b.** Attach the template to Cisco SD-WAN Validator. **8.** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, and verify that the Cisco SD-WAN Validator is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**, and verify that the Cisco SD-WAN Validator is operational.

Bring-Up Task	Step-by-Step Procedure
Step 3: Start the Cisco Catalyst SD-WAN Controller.	**1.** On the hypervisor, create a VM instance. **2.** Boot the Cisco SD-WAN Controller server and start the VM. **3.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controller**, add Cisco Catalyst SD-WAN Controller and generate the CSR. **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. **4.** Check for a confirmation email from Symantec that your request has been received. **5.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **6.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, check that the certificate has been installed. **7.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for Cisco Catalyst SD-WAN Controller. **b.** Attach the template to Cisco Catalyst SD-WAN Controller. **8.** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, and verify that Cisco Catalyst SD-WAN Controller is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**, and verify that Cisco Catalyst SD-WAN Controller is operational.
Step 4: Configure the router.	**1.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**, upload the router authorized serial number file. **2.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, check that the router's chassis and serial number are in the list. **3.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, authorize each router by marking it Valid in the Validity column. **4.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **WAN Edge List**, send the WAN Edge list to the controller devices. **5.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for the router. **b.** Attach the template to the router.

Bring-Up Task	Step-by-Step Procedure
Step 5: Connect AC power and boot a hardware router.	**1.** Connect AC power to the router. **2.** If needed, flip the On/Off switch on the rear of the router to the ON position. **3.** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** or choose **Monitor** > **Devices** > **Device Dashboard**, verify that the router is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** or choose **Monitor** > **Network** > **Device Dashboard**, verify that the router is operational.

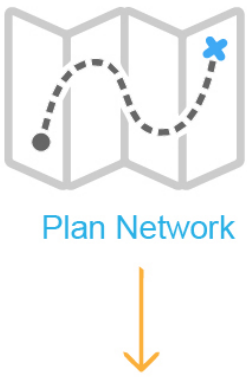
Summary of the User Portion of the Bring-Up Sequence

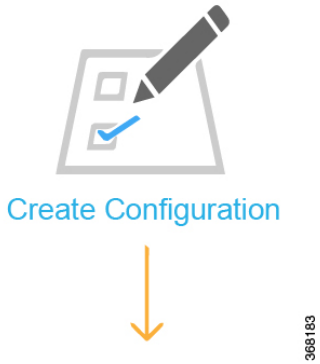
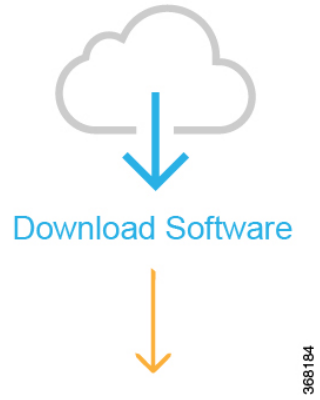
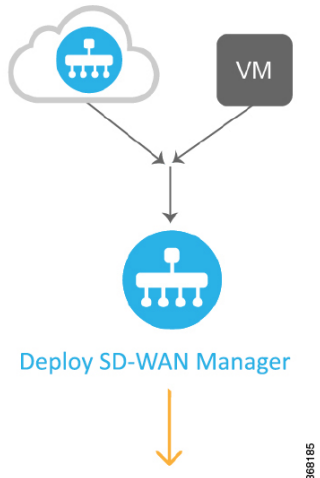
Generally, what you do to bring up the Cisco Catalyst SD-WAN overlay network is what you do to bring up any network. You plan out the network, create device configurations, and then deploy the network hardware and software components. These components include all the Cisco vEdge devices, all the traditional routers that participate in the overlay network, and all the network devices that provide shared services across the overlay network, such as firewalls, load balancers, and IDP systems.

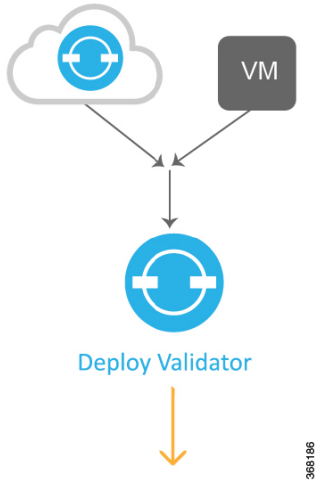
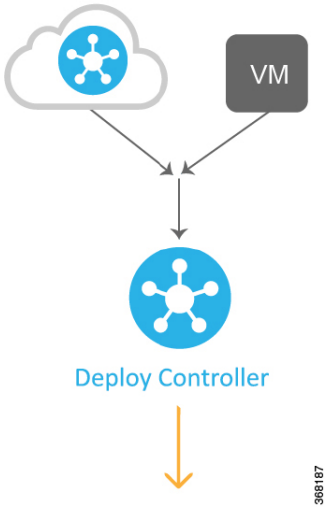
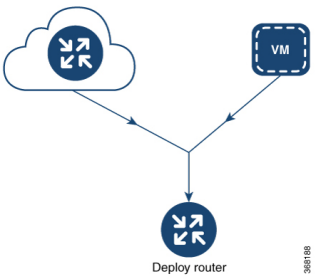
The following table summarizes the steps for the user portion of the Cisco Catalyst SD-WAN overlay network bring-up sequence. The details of each step are provided in the articles that are listed in the **Procedure** column. While you can bring up the Cisco vEdge devices in any order, it is recommended that you deploy them in the order listed below, which is the functional order in which the devices verify and authenticate themselves.

If your network has firewall devices, see Firewall Ports for Cisco Catalyst SD-WAN Deployments.

Table 24:

	Workflow	Procedure
1		Plan out your overlay network. See Components of the Cisco Catalyst SD-WAN Solution.

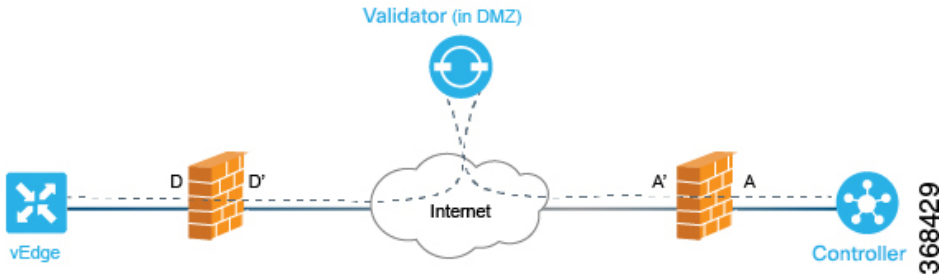
	Workflow	Procedure
2		On paper, create device configurations that implement the desired architecture and functionality. See the Software documentation for your software release.
3		Download the software images.
4		Deploy Cisco SD-WAN Manager in the data center: 1. Create a Cisco SD-WAN Manager VM instance, either on an ESXi or a KVM hypervisor. 2. Create either a minimal or a full configuration for each Cisco SD-WAN Manager server. 3. Configure certificate settings and generate a certificate for Cisco SD-WAN Manager. 4. Create a Cisco SD-WAN Manager cluster.

	Workflow	Procedure
5		Deploy the Cisco SD-WAN Validator: 1. Create a Cisco SD-WAN Validator VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the Cisco SD-WAN Validator. 3. Add the Cisco SD-WAN Validator to the overlay network. During this process, you generate a certificate for the Cisco SD-WAN Validator. 4. Create a full configuration for the Cisco SD-WAN Validator.
6		Deploy the Cisco SD-WAN Controller in the data center: 1. Create a Cisco SD-WAN Controller VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the Cisco SD-WAN Controller. 3. Add the Cisco SD-WAN Controller to the overlay network. During this process, you generate a certificate for the Cisco SD-WAN Controller. 4. Create a full configuration for the Cisco SD-WAN Controller.
7		Deploy the Cisco vEdge routers in the overlay network: 1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor. 2. For software vEdge Cloud routers, send a certificate signing request to Symantec and then install the signed certificate on the router. 3. From Cisco SD-WAN Manager, send the serial numbers of all Cisco vEdge routers to the Cisco SD-WAN Controller and Cisco SD-WAN Validator in the overlay network. 4. Create a full configuration for the Cisco vEdge routers.

Automatic Portions of the Bring-Up Sequence

After the Cisco vEdge devices boot and start running with their initial configurations, the second part of the bring-up process begins automatically. This automatic process is led by the Cisco SD-WAN Validator, as illustrated in the figure below. Under the leadership of the Cisco SD-WAN Validator software, the Cisco vEdge devices set up encrypted communication channels between themselves. Over these channels, the devices automatically validate and authenticate each other, a process that establishes an operational overlay network. Once the overlay network is running, the Cisco vEdge devices automatically receive and activate their full configurations from the Cisco SD-WAN Manager server. (The exception is the Cisco SD-WAN Manager. You must manually configure each Cisco SD-WAN Manager server itself).

Figure 11: Cisco SD-WAN Validator Automated Bring-Up Sequence



The following sections explain what happens under the covers, during the automatic portion of the bring-up process. This explanation is provided to help you understand the detailed workings of the Cisco Catalyst SD-WAN software so that you can better appreciate the means by which the Cisco Catalyst SD-WAN solution creates a highly secure overlay framework to support your networking requirements.

User Input Required for the ZTP Automatic Authentication Process

The automatic validation and authentication of Cisco vEdge devices that occurs during the bringup process can happen only if Cisco SD-WAN Controllers and Cisco SD-WAN Validators know the serial and chassis numbers of the devices that are permitted in the network. Let's first define these two terms:

- Serial number—Each Cisco vEdge device has a serial number, which is a 40-byte number that is included in the device's certificate. For Cisco SD-WAN Validator and Cisco SD-WAN Controller, the certificate can be provided by Symantec or by an enterprise root CA. For the vEdge routers, the certificate is provided in the hardware's trusted board ID chip.
- Chassis number—In addition to a serial number, each vEdge router is identified by a chassis number. Because the vEdge router is the only Cisco SD-WAN Controller manufactured hardware, it is the only Cisco vEdge device that has a chassis number. There is a one-to-one mapping between a vEdge router's serial number and its chassis number.

The Cisco SD-WAN Controllers and Cisco SD-WAN Validators learn the serial and chassis numbers during the initial configuration of these devices:

- Cisco SD-WAN Controller authorized serial numbers—The Cisco SD-WAN Manager learns the serial numbers for all Cisco SD-WAN Controllers that are allowed to be in the network while it is creating a CSR and installing the signed certificate. You download these serial numbers to Cisco SD-WAN Validator, and Cisco SD-WAN Validator pushes them to the Cisco Catalyst SD-WAN Controller during the automatic authentication process.

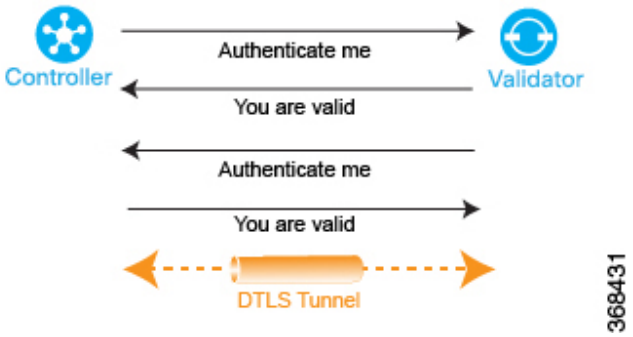
- vEdge authorized serial number file—This file contains the serial and chassis numbers of all the vEdge routers that are allowed to be in the network. You upload this file to Cisco SD-WAN Validators and Cisco SD-WAN Controllers.

In addition to the device serial and chassis numbers, the automatic validation and authentication procedure depends on having each device configured with the same organization name. You configure this name on Cisco SD-WAN Manager, and it is included in the configuration file on all devices. The organization name must be identical on all the devices that belong to a single organization (the name is case-sensitive). The organization name is also included in the certificate for each device, which is created either by Cisco Catalyst SD-WAN or by an enterprise root CA.

Authentication between Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Validator

From a functional point of view, the first two devices on the Cisco Catalyst SD-WAN overlay network that validate and authenticate each other are Cisco SD-WAN Controller and Cisco SD-WAN Validator. This process is initiated by Cisco SD-WAN Controller.

Figure 12: Authentication of Cisco SD-WAN Controller and Cisco SD-WAN Validator



When Cisco SD-WAN Controller comes up, it initiates a connection to Cisco SD-WAN Validator, which is how Cisco SD-WAN Validator learns about Cisco SD-WAN Controller. These two devices then automatically begin a two-way authentication process—Cisco SD-WAN Controller authenticates itself with , and Cisco SD-WAN Validator authenticates itself with Cisco SD-WAN Validator. The two-way handshaking between the two devices during the authentication process occurs in parallel. However, for clarity, the figure here, which is a high-level representation of the authentication steps, illustrates the handshaking sequentially. If the authentication handshaking succeeds, a permanent DTLS communication channel is established between the Cisco SD-WAN Controller and Cisco SD-WAN Validator devices. If any one of the authentication steps fails, the device noting the failure tears down the connection between the two devices, and the authentication attempt terminates.

The Cisco SD-WAN Controller knows how to reach Cisco SD-WAN Validator, because one of the parameters that you provision when you configure it is the IP address or DNS name of Cisco SD-WAN Validator. Cisco SD-WAN Validator is primed to respond to requests from Cisco SD-WAN Validator because:

- It knows that its role is to be the authentication system, because you included this information in the Cisco SD-WAN Validator configuration.
- You downloaded the Cisco SD-WAN Controller authorized serial numbers from Cisco SD-WAN Manager to Cisco SD-WAN Validator.

If Cisco SD-WAN Validator has not yet started when Cisco SD-WAN Controller initiates the authentication process, Cisco SD-WAN Controller periodically attempts to initiate a connection until it is successful.

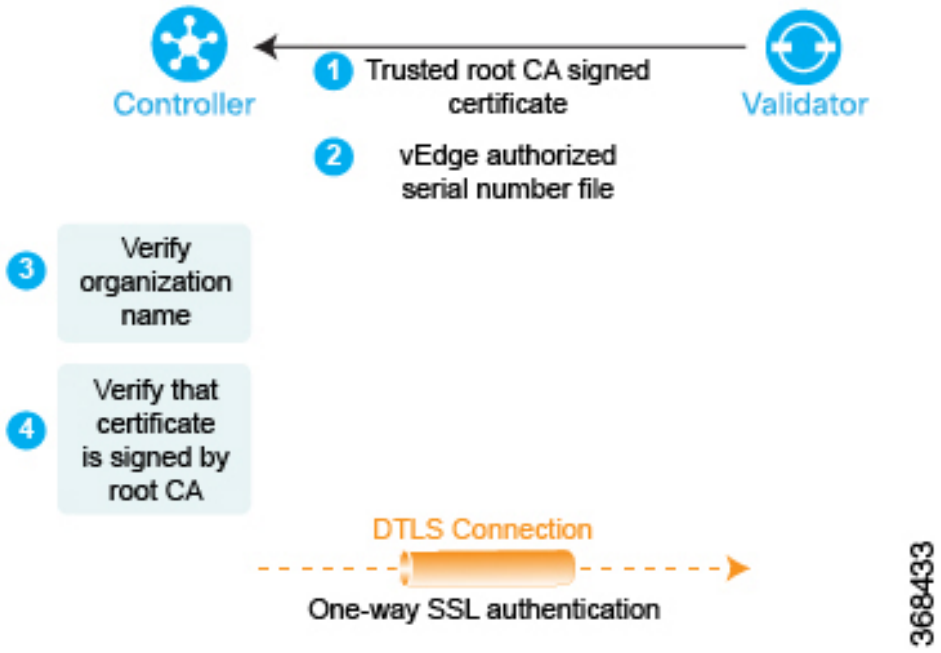
Below is a more detailed step-by-step description of how the automatic authentication occurs between Cisco SD-WAN Controller and Cisco SD-WAN Validator.

To initiate a session between Cisco SD-WAN Controller and Cisco SD-WAN Validator, Cisco SD-WAN Controller initiates an encrypted DTLS connection to Cisco SD-WAN Validator. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots.

Over this encrypted channel, Cisco SD-WAN Controller and Cisco SD-WAN Validator authenticate each other. Each device authenticates the other in parallel. For our discussion, let's start with Cisco SD-WAN Controller authentication of Cisco SD-WAN Validator:

1. Cisco SD-WAN Validator sends its trusted root CA signed certificate to the Cisco SD-WAN Controller.
2. Cisco SD-WAN Validator sends the vEdge authorized serial number file to the Cisco SD-WAN Controller.
3. Cisco SD-WAN Controller uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on Cisco SD-WAN Controller. If the two organization names match, Cisco SD-WAN Controller knows that the organization of Cisco SD-WAN Validator is proper. If they do not match, Cisco Catalyst SD-WAN Controller tears down the DTLS connection.
4. Cisco Catalyst SD-WAN Controller uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, Cisco Catalyst SD-WAN Controller knows that the certificate itself is valid. If the signature is incorrect, Cisco Catalyst SD-WAN Controller tears down the DTLS connection.

Figure 13: Cisco SD-WAN Controller authenticates Cisco SD-WAN Validator

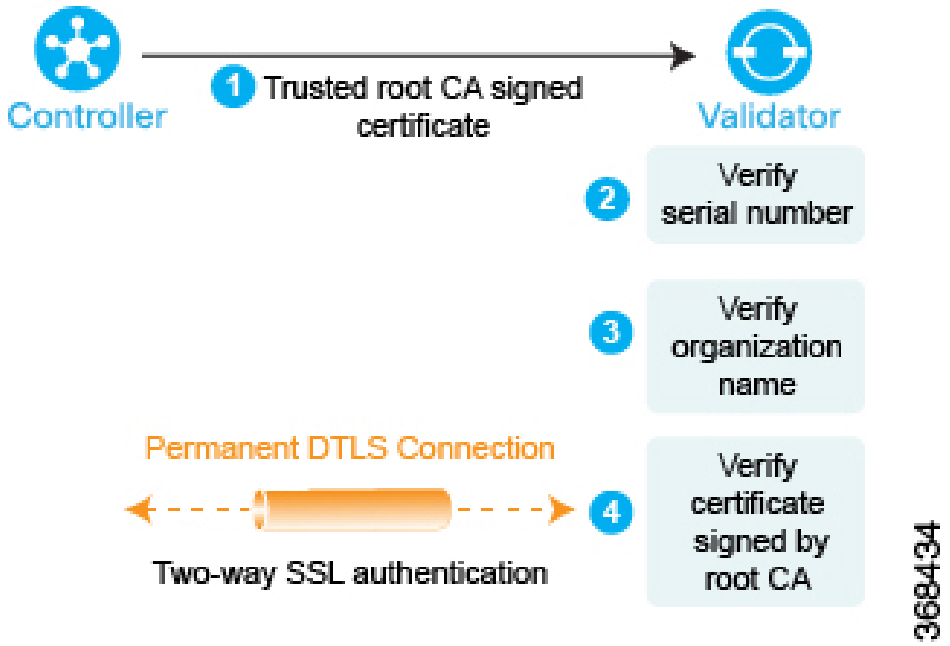


After performing these two checks, Cisco SD-WAN Controller authentication of Cisco SD-WAN Validator is complete.

In the other direction, Cisco SD-WAN Validator authenticates Cisco SD-WAN Controller:

1. Cisco SD-WAN Controller sends its trusted root CA signed certificate to Cisco SD-WAN Validator.
2. Cisco SD-WAN Validator uses its chain of trust to extract Cisco SD-WAN Controller serial number from the certificate. The number must match one of the numbers in the Cisco SD-WAN Controller authorized serial number file. If there is no match, Cisco SD-WAN Validator tears down the DTLS connection.
3. Cisco SD-WAN Validator uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on Cisco SD-WAN Validator. If the two organization names match, the Cisco SD-WAN Validator knows that the organization of Cisco SD-WAN Controller is proper. If they do not match, Cisco SD-WAN Validator tears down the DTLS connection.
4. The Cisco SD-WAN Validator uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, Cisco SD-WAN Validator knows that the certificate itself is valid. If the signature is incorrect, Cisco SD-WAN Validator tears down the DTLS connection.

Figure 14: Cisco SD-WAN Validator authenticates Cisco SD-WAN Controller



After performing these three checks, the Cisco SD-WAN Validator authentication of Cisco SD-WAN Validator is complete.

After the bidirectional authentication completes between the two devices, the DTLS connection between Cisco SD-WAN Validator and Cisco SD-WAN Controller transitions from being a temporary connection to being a permanent connection, and the two devices establish an OMP session over the connection.

In a domain that has multiple Cisco SD-WAN Controllers for redundancy, this process repeats between each pair of Cisco SD-WAN Controller and Cisco SD-WAN Validator devices. In coordination with Cisco SD-WAN Validator, Cisco SD-WAN Controllers learn about each other and they synchronize their route information. It is recommended that you connect the different Cisco SD-WAN Controller to the WAN network through different NAT devices for higher availability.

A Cisco SD-WAN Validator has only as many permanent DTLS connections as the number of Cisco SD-WAN Controllers in the network topology. These DTLS connections are part of the network's control plane; no data traffic flows over them. After all Cisco SD-WAN Controllers have registered themselves with Cisco SD-WAN Validator, Cisco SD-WAN Validator and Cisco SD-WAN Controllers are ready to validate and authenticate the vEdge routers in the Cisco Catalyst SD-WAN network.

Authentication Between Cisco Catalyst SD-WAN Controllers

In a domain with multiple Cisco SD-WAN Controllers, the controllers must authenticate each other so that they can establish a full mesh of permanent DTLS connection between themselves for synchronizing OMP routes. Cisco SD-WAN Controller learns the IP address of the other Cisco SD-WAN Controller from Cisco SD-WAN Validator.

Cisco SD-WAN Controller learns about the possibility of other Cisco SD-WAN Controllers being present on the network during the authentication handshaking with the Cisco SD-WAN Validator, when it receives a copy of the Cisco SD-WAN Controller authorized serial number file. If this file has more than one serial number, it indicates that the network may, at some point, have multiple Cisco SD-WAN Controllers.

As one Cisco SD-WAN Controller authenticates with Cisco SD-WAN Validator, Cisco SD-WAN Validator sends Cisco SD-WAN Controller the IP address of other Cisco SD-WAN Controllers it has authenticated with. If Cisco SD-WAN Validator later learns of another Cisco SD-WAN Controller, it sends that controller's address to the other already authenticated Cisco SD-WAN Controllers.

Then, Cisco SD-WAN Controllers perform the steps below to authenticate each other. Again, each device authenticates the other in parallel, but for clarity, we describe the process sequentially.

1. Cisco SD-WAN Controller1 (vSmart1) initiates an encrypted DTLS connection to Cisco SD-WAN Controller2 (vSmart2) and sends its trusted root CA signed certificate to Cisco SD-WAN Controller2.
2. Cisco SD-WAN Controller2 uses its chain of trust to extract the Cisco SD-WAN Controller1's serial number. The number must match one of the numbers in the Cisco SD-WAN Controller authorized serial number file. If there is no match, Cisco SD-WAN Controller2 tears down the DTLS connection.
3. Cisco SD-WAN Controller2 uses its chain of trust to extract the organization name from the certificate and compares it to the locally configured organization name. If the two organization names match, Cisco SD-WAN Controller2 knows that the organization of Cisco SD-WAN Controller1 is proper. If they do not match, Cisco SD-WAN Controller2 tears down the DTLS connection.
4. Cisco SD-WAN Controller2 uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, Cisco SD-WAN Controller2 knows that the certificate itself is valid. If the signature is incorrect, Cisco SD-WAN Controller2 tears down the DTLS connection.

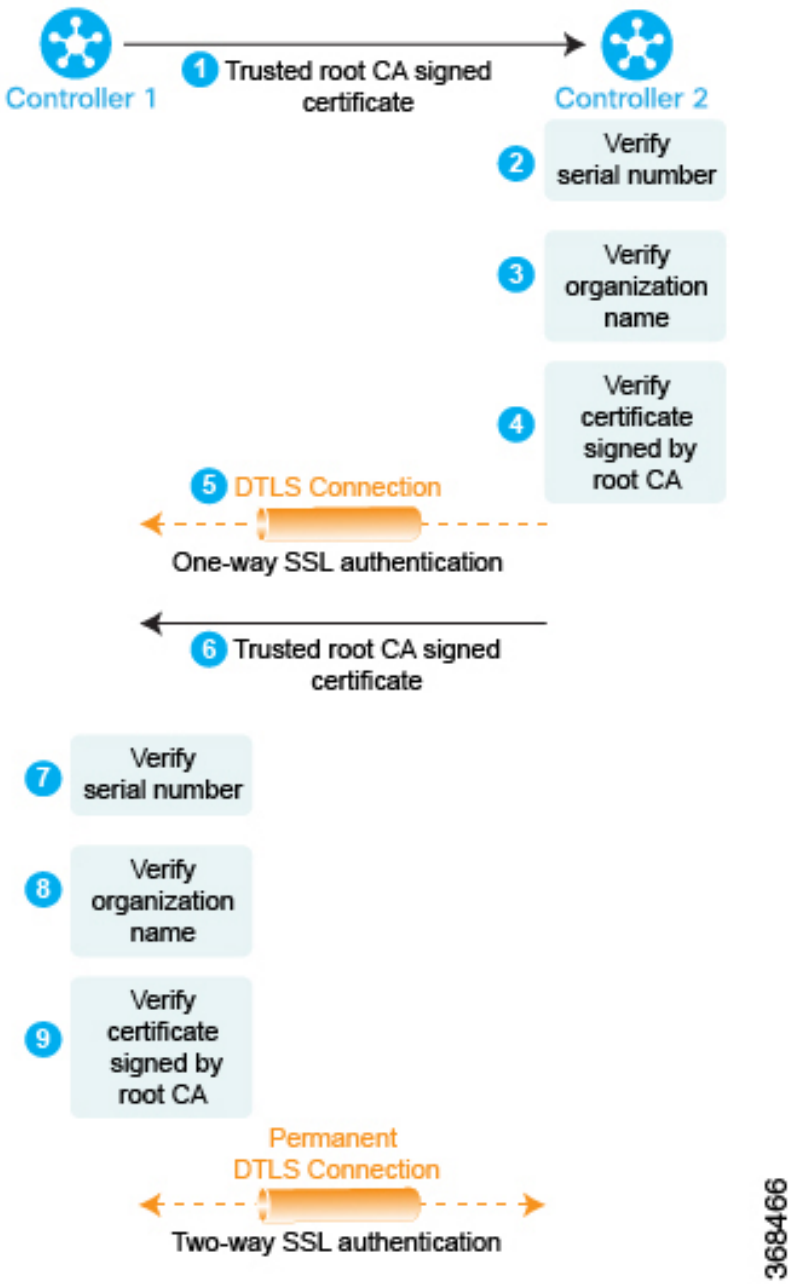
After performing these three checks, Cisco SD-WAN Controller2 authentication of Cisco SD-WAN Controller1 is complete.

Now, Cisco SD-WAN Controller1 authenticates Cisco SD-WAN Controller2, performing the same steps as above.

1. First, Cisco SD-WAN Controller2 sends its trusted root CA signed certificate to Cisco SD-WAN Controller1.
2. Cisco SD-WAN Controller1 uses its chain of trust to extract the Cisco SD-WAN Controller2's serial number. The number must match one of the numbers in the Cisco SD-WAN Controller authorized serial number file. If there is no match, Cisco SD-WAN Controller1 tears down the DTLS connection.

3. Cisco SD-WAN Controller1 uses its chain of trust to extract the organization name from the certificate and compares it to the locally configured organization name. If the two organization names match, Cisco SD-WAN Controller2 knows that the organization of Cisco SD-WAN Controller2 is proper. If they do not match, Cisco SD-WAN Controller1 tears down the DTLS connection.
4. Cisco SD-WAN Controller1 uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, Cisco SD-WAN Controller2 knows that the certificate itself is valid. If the signature is incorrect, Cisco SD-WAN Controller1 tears down the DTLS connection.

Figure 15: Authentication of Cisco SD-WAN Controller



After performing these three checks, Cisco SD-WAN Controller1 authentication of Cisco SD-WAN Controller2 is complete, and the temporary DTLS connection between the two devices becomes permanent.

After all the Cisco SD-WAN Controllers have registered themselves with , Cisco SD-WAN Validator and Cisco SD-WAN Controllers are ready to validate and authenticate the vEdge routers in the Cisco Catalyst SD-WAN network.

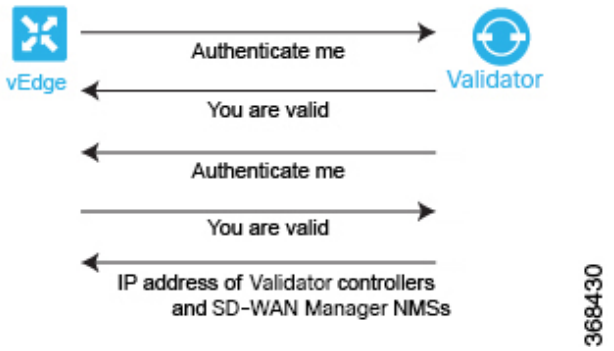
Authentication between Cisco Catalyst SD-WAN Validator and a Cisco vEdge Router

When you deploy a Cisco vEdge router in the network, it first needs to do two things:

- Establish a secure connection with Cisco SD-WAN Manager so that it can receive its full configuration.
- Establish a secure connection with Cisco Catalyst SD-WAN Controller can begin participating in the Cisco Catalyst SD-WAN overlay network.

When a Cisco vEdge device comes up, how does it automatically discover Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller and establish connections with them? It does so with help from Cisco SD-WAN Validator. The initial configuration on the Cisco vEdge router contains the Cisco SD-WAN Validator system's IP address (or DNS name). Using this information, the Cisco vEdge router establishes a DTLS connection with Cisco SD-WAN Validator, and the two devices authenticate each other to confirm that they are valid Cisco vEdge devices. Again, this authentication is a two-way process that happens automatically. When the authentication completes successfully, Cisco SD-WAN Validator sends the Cisco vEdge router the IP addresses of Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller. Then, the Cisco vEdge router tears down its connection with Cisco SD-WAN Validator and begins establishing secure DTLS connections with the othe two devices.

Figure 16: Automatic Authentication of Cisco vEdge Router and Cisco SD-WAN Validator



After you boot Cisco vEdge routers and manually perform the initial configuration, they automatically start looking for their Cisco SD-WAN Validator. Cisco SD-WAN Validator and Cisco SD-WAN Controllers are able to recognize and authenticate the Cisco vEdge routers in part because you have installed the Cisco vEdge authorized device list file on both these devices.

After you boot a Cisco vEdge router, you manually perform the initial configuration, at a minimum setting the IP address of DNS name of Cisco SD-WAN Validator. The Cisco vEdge router uses this address information to reach Cisco SD-WAN Validator. Cisco SD-WAN Validator is primed to respond to requests from a Cisco vEdge router because:

- It knows that its role is to be the authentication system, because you included this information in the initial Cisco SD-WAN Validator configuration.
- As part of the initial configuration, you installed the Cisco vEdge authorized serial number file on Cisco SD-WAN Validator.

If Cisco SD-WAN Validator has not yet started when a Cisco vEdge router initiates the authentication process, the Cisco vEdge router periodically attempts to initiate a connection until the attempt succeeds.

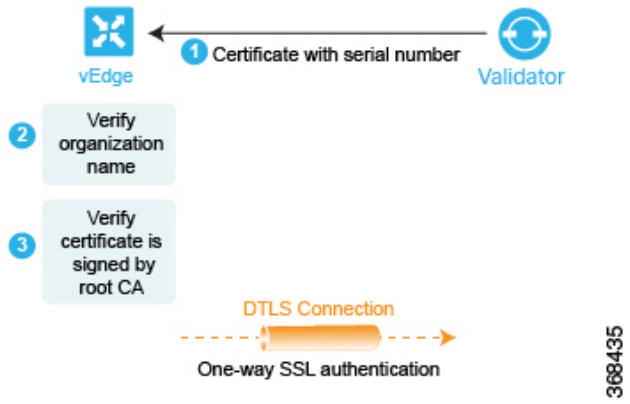
Below is a more detailed step-by-step description of how the automatic authentication occurs between Cisco SD-WAN Validator and a Cisco vEdge router.

First, the Cisco vEdge router initiates an encrypted DTLS connection to the public IP address of Cisco SD-WAN Validator. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots. Cisco SD-WAN Validator receives the Cisco vEdge router's original interface address and uses the outer IP address in the received packet to determine whether the Cisco vEdge router is behind a NAT. If it is, Cisco SD-WAN Validator creates a mapping of the Cisco vEdge router's public IP address and port to its private IP address.

Over this encrypted DTLS channel, the Cisco vEdge router and Cisco SD-WAN Validator proceed to authenticate each other. As with other device authentication, the Cisco vEdge router and Cisco SD-WAN Validator authenticate each other in parallel. We start our discussion by describing how the Cisco vEdge router authenticates Cisco SD-WAN Validator:

1. Cisco SD-WAN Validator sends its trusted root CA signed certificate to the Cisco vEdge router.
2. The Cisco vEdge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the router itself. If the two organization names match, the Cisco vEdge routers knows that the organization of Cisco SD-WAN Validator is proper. If they do not match, the Cisco vEdge router tears down the DTLS connection.
3. The Cisco vEdge router uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, the Cisco vEdge router knows that the certificate itself is valid. If the signature is incorrect, the Cisco vEdge router tears down the DTLS connection.

Figure 17: Cisco vEdge router authenticates Cisco SD-WAN Validator



After performing these two checks, the Cisco vEdge router knows that Cisco SD-WAN Validator is valid, and its authentication of Cisco SD-WAN Validator is complete.

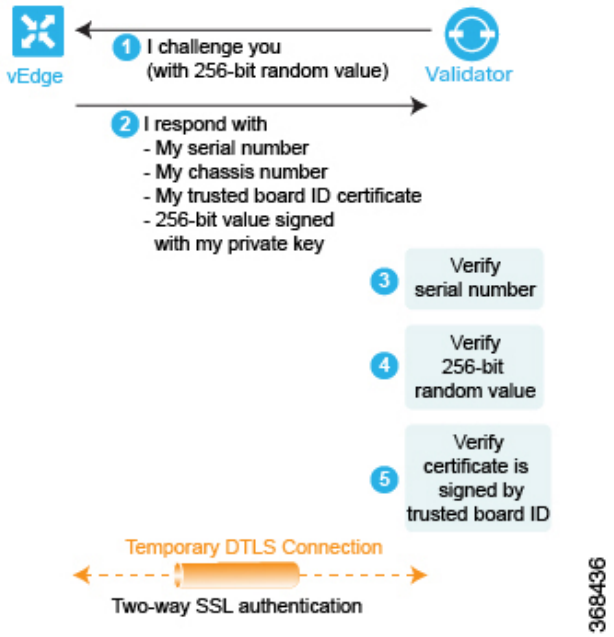
In the opposite direction, Cisco SD-WAN Validator authenticates the Cisco vEdge router:

1. Cisco SD-WAN Validator sends a challenge to the Cisco vEdge router. The challenge is a 256-bit random value.
2. The Cisco vEdge router sends a response to the challenge that includes the following:
   - Cisco vEdge serial number
   - Cisco vEdge chassis number

- Cisco vEdge board ID certificate
- 256-bit random value signed by the Cisco vEdge router's private key

3. Cisco SD-WAN Validator compares the serial and chassis numbers to the list in its Cisco vEdge authorized device list file. The numbers must match one of the number pairs in the file. If there is no match, Cisco SD-WAN Validator tears down the DTLS connection.
4. Cisco SD-WAN Validator checks that the signing of the 256-bit random value is proper. It does this using the Cisco vEdge router's public key, which it extracts from the router's board ID certificate. If the signing is not correct, Cisco SD-WAN Validator tears down the DTLS connection.
5. Cisco SD-WAN Validator uses the root CA chain from the Cisco vEdge routers board ID certificate to validate that the board ID certificate is itself valid. If the certificate is not valid, Cisco SD-WAN Validator tears down the DTLS connection.

Figure 18: Cisco SD-WAN Validator authenticates Cisco vEdge router



After performing these three checks, Cisco SD-WAN Validator knows that Cisco vEdge router is valid, and its authentication of the router is complete.

When the two-way authentication succeeds, Cisco SD-WAN Validator performs the final step of its orchestration, sending messages to the Cisco vEdge router and Cisco Catalyst SD-WAN Controller in parallel. To the Cisco vEdge router, Cisco SD-WAN Validator sends the following:

- The IP addresses of Cisco SD-WAN Controllers in the network so that the Cisco vEdge router can initiate connections to them. The address can be public IP addresses, or for the controllers that are behind a NAT gateway, the addresses are a list of the public and private IP addresses and port numbers. If the Cisco vEdge router is behind a NAT gateway, Cisco SD-WAN Validator requests that the Cisco vEdge router initiate a session with Cisco Catalyst SD-WAN Controller.
- Serial numbers of Cisco SD-WAN Controllers that are authorized to be in the network.

To Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Validator sends the following:

- A message announcing the new Cisco vEdge router in the domain.
- If the Cisco vEdge router is behind a NAT gateway, Cisco SD-WAN Validator sends a request to Cisco Catalyst SD-WAN Controller to initiate a session with the Cisco vEdge router.

Then, the Cisco vEdge router tears down the DTLS connection with the Cisco SD-WAN Validator.

Authentication between the Cisco vEdge Router and Cisco SD-WAN Manager

After the Cisco vEdge router and Cisco SD-WAN Validator have authenticated each other, the Cisco vEdge router receives its full configuration over a DTLS connection with Cisco SD-WAN Manager:

1. The Cisco vEdge router establishes a DTLS connection with Cisco SD-WAN Manager.
2. Cisco SD-WAN Manager server sends the configuration file to the Cisco vEdge router.
3. When the Cisco vEdge router receives the configuration file and activates its full configuration.
4. The Cisco vEdge router starts advertising prefixes to Cisco SD-WAN Controller.

If you are not using Cisco SD-WAN Manager, you can log in to the Cisco vEdge router and either manually load its configuration file or manually configure the router.

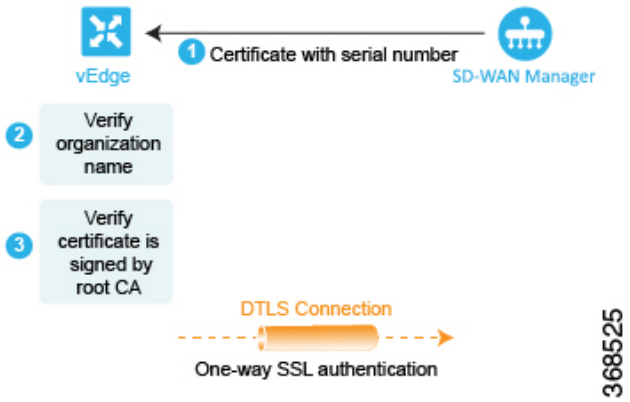
Below is a more detailed step-by-step description of how the automatic authentication occurs between a Cisco vEdge router and Cisco SD-WAN Manager.

First, the Cisco vEdge router initiates an encrypted DTLS connection to the IP address of Cisco SD-WAN Manager. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots. Cisco SD-WAN Manager receives the Cisco vEdge router's original interface address and uses the outer IP address in the received packet to determine whether the Cisco vEdge router is behind a NAT. If it is, Cisco SD-WAN Manager creates a mapping of the Cisco vEdge router's public IP address and port to its private IP address.

Over this encrypted DTLS channel, the Cisco vEdge router and Cisco SD-WAN Manager proceed to authenticate each other. As with other device authentication, the Cisco vEdge router and Cisco SD-WAN Manager authenticate each other in parallel. We start our discussion by describing how the Cisco vEdge router authenticates Cisco SD-WAN Manager:

1. Cisco SD-WAN Manager sends its trusted root CA signed certificate to the Cisco vEdge router.
2. The Cisco vEdge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the router itself. If the two organization names match, the Cisco vEdge routers knows that the organization of Cisco SD-WAN Manager is proper. If they do not match, the Cisco vEdge router tears down the DTLS connection.
3. The Cisco vEdge router uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, the Cisco vEdge router knows that the certificate itself is valid. If the signature is incorrect, the Cisco vEdge router tears down the DTLS connection.

Figure 19: Cisco vEdge Router Authenticates Cisco SD-WAN Manager

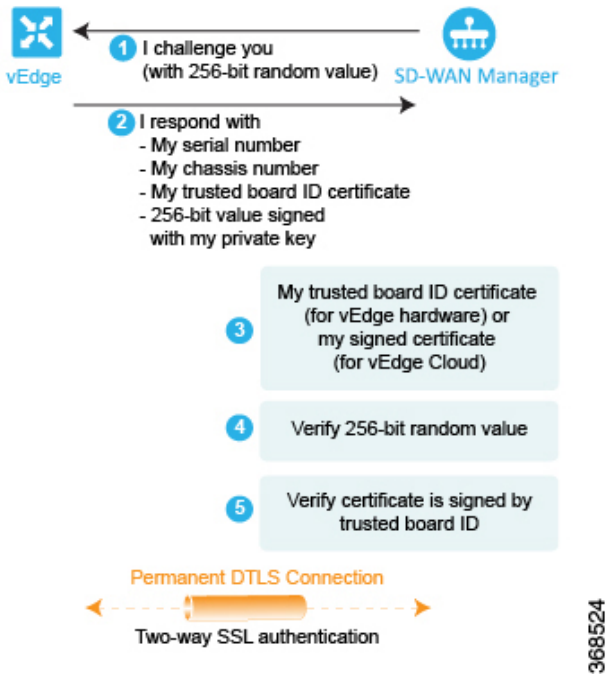


After performing these two checks, the Cisco vEdge router knows that Cisco SD-WAN Manager is valid, and its authentication of Cisco SD-WAN Manager is complete.

In the opposite direction, Cisco SD-WAN Manager authenticates the Cisco vEdge router:

1. Cisco SD-WAN Manager sends a challenge to the Cisco vEdge router. The challenge is a 256-bit random value.
2. The Cisco vEdge router sends a response to the challenge that includes the following:
   - Cisco vEdge serial number
   - Cisco vEdge chassis number
   - Cisco vEdge board ID certificate (for a hardware Cisco vEdge router) or the signed certification (for a Cisco vEdge Cloud router)
   - 256-bit random value signed by the Cisco vEdge router's private key
3. Cisco SD-WAN Manager compares the serial and chassis numbers to the list in its Cisco vEdge authorized device list file. The numbers must match one of the number pairs in the file. If there is no match, Cisco SD-WAN Managerthe Cisco SD-WAN Manager NMS tears down the DTLS connection.
4. Cisco SD-WAN Manager checks that the signing of the 256-bit random value is proper. It does this using the Cisco vEdge router's public key, which it extracts from the router's board ID certificate. If the signing is not correct, Cisco SD-WAN Manager tears down the DTLS connection.
5. Cisco SD-WAN Manager uses the root CA chain from the Cisco vEdge routers board ID certificate to validate that the board ID certificate is itself valid. If the certificate is not valid, Cisco SD-WAN Manager tears down the DTLS connection.

Figure 20: Cisco SD-WAN Manager Authenticates Cisco vEdge Router



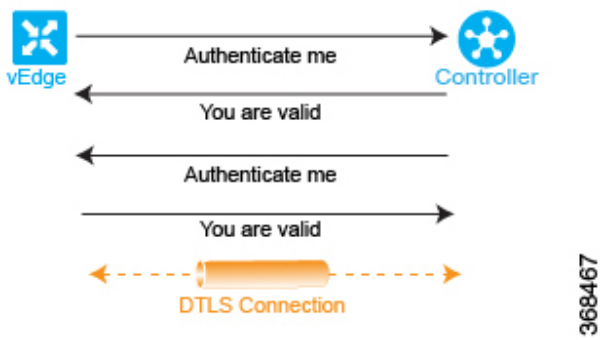
After performing these three checks, Cisco SD-WAN Manager knows that Cisco vEdge router is valid, and its authentication of the router is complete.

When the two-way authentication succeeds, Cisco SD-WAN Manager server sends the configuration file to the Cisco vEdge router. When the Cisco vEdge router receives the configuration file, it activates its full configuration and starts advertising prefixes to Cisco SD-WAN Controller.

Authentication between Cisco Catalyst SD-WAN Controller and the Cisco vEdge Router

The last step in the automatic authentication process is for Cisco SD-WAN Controller and the Cisco vEdge router to authenticate each other. In this step, Cisco SD-WAN Controller performs authentication to ensure that the Cisco vEdge router belongs in its network, and the Cisco vEdge router also authenticates Cisco SD-WAN Controller. When the authentication completes, the DTLS connection between the two devices becomes permanent, and Cisco SD-WAN Controller establishes an OMP peering session running over the DTLS connection. Then, the Cisco vEdge router starts sending data traffic over the Cisco Catalyst SD-WAN overlay network.

Figure 21: Authentication of Cisco SD-WAN Controller and Cisco Cisco vEdge Router



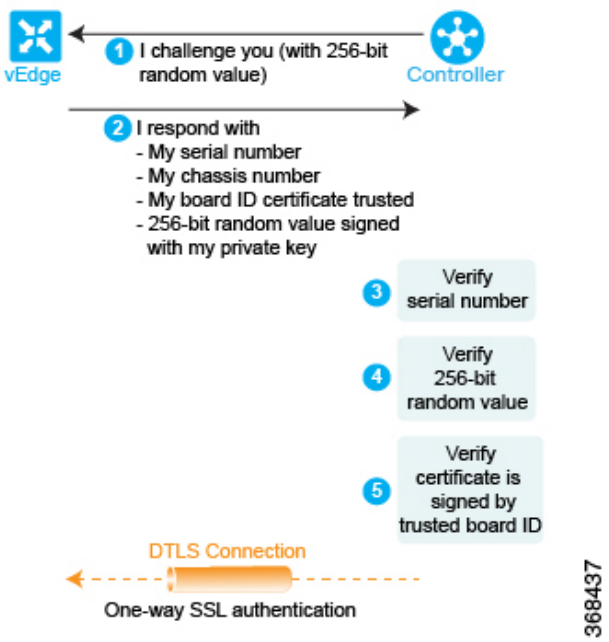
In this section below, is a more detailed step-by-step description of how the automatic authentication occurs between Cisco SD-WAN Controller and a Cisco vEdge router.

To initiate a session between Cisco SD-WAN Controller and a Cisco vEdge router, one of the two devices initiates an encrypted DTLS connection to the other. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots.

The authentication between Cisco SD-WAN Controller and a Cisco vEdge router is a two-way process that occurs in parallel. Let's start our discussion with how Cisco SD-WAN Controller authenticates a Cisco vEdge router:

1. Cisco SD-WAN Controller sends a challenge to the Cisco vEdge router. The challenge is a 256-bit random value.
2. The Cisco vEdge router sends a response to the challenge that includes the following:
   - Cisco vEdge serial number
   - Cisco vEdge chassis number
   - Cisco vEdge board ID certificate
   - 256-bit random value signed by the Cisco vEdge router's private key
3. Cisco SD-WAN Controller compares the serial and chassis numbers to the list in its Cisco vEdge authorized device list file. The numbers must match one of the number pairs in the file. If there is no match, Cisco SD-WAN Controller tears down the DTLS connection.
4. Cisco SD-WAN Controller checks that the signing of the 256-bit random value is proper. It does this using the Cisco vEdge router's public key, which it extracts from the router's board ID certificate. If the signing is not correct, Cisco SD-WAN Controller tears down the DTLS connection.
5. Cisco SD-WAN Controller uses the root CA chain from the Cisco vEdge routers board ID certificate to validate that the board ID certificate is itself valid. If the certificate is not valid, Cisco SD-WAN Controller tears down the DTLS connection.
6. Cisco SD-WAN Controller compares the response with the original challenge. If the response matches the challenge that Cisco SD-WAN Validator issued, authentication between the two devices occurs. Otherwise, Cisco SD-WAN Controller tears down the DTLS connection.

Figure 22: Cisco SD-WAN Controller authenticates a Cisco vEdge router

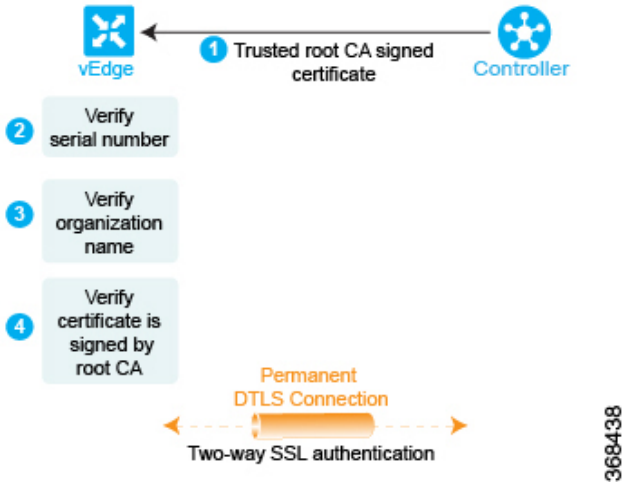


After performing these three checks, Cisco SD-WAN Controller knows that Cisco vEdge router is valid, and its authentication of the router is complete.

In the other direction, the Cisco vEdge router authenticates Cisco SD-WAN Controller:

1. Cisco SD-WAN Controller sends its trusted root CA signed certificate to the Cisco vEdge router.
2. The Cisco vEdge router uses its chain of trust to extract Cisco SD-WAN Controller's serial number from the certificate. The number must match one of the numbers in the Cisco SD-WAN Controller authorized serial number file. If there is no match, the Cisco vEdge router tears down the DTLS connection.
3. The Edge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the Cisco vEdge router. If the two organization names match, the Cisco vEdge router knows that the organization of Cisco SD-WAN Controller is proper. If they do not match, the Cisco vEdge router tears down the DTLS connection.
4. The Cisco vEdge router uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, the Cisco vEdge router knows that the certificate itself is valid. If the signature is incorrect, the Cisco vEdge router tears down the DTLS connection.

Figure 23: Cisco vEdge Router authenticates Cisco SD-WAN Controller



After performing these three checks, the Cisco vEdge authentication of Cisco SD-WAN Controller is complete. The DTLS connection that is used for authentication now becomes a permanent (nontransient) connection, and the two devices establish an OMP session over it that is used to exchange control plane traffic.

This authentication procedure repeats for each Cisco SD-WAN Controller and each Cisco vEdge router that you introduce into the overlay network.

Each Cisco vEdge router in the network must connect to at least one Cisco SD-WAN Controller. That is, a DTLS connection must be successfully established between each Cisco vEdge router and one Cisco SD-WAN Controller. The Cisco SD-WAN network has the notion of a domain. Within a domain, it is recommended that you have multiple Cisco SD-WAN Controllers for redundancy. Then each Cisco vEdge router can connect to more than one Cisco SD-WAN Controller.

Over the OMP session, a Cisco vEdge router relays various control plane–related information to Cisco SD-WAN Controller so that Cisco SD-WAN Controller can learn the network topology:

- The Cisco vEdge router advertises the service-side prefixes and routes that it has learned from its local static and dynamic (BGP and OSPF) routing protocols.
- Each Cisco vEdge router has a transport address, called a TLOC, or transport location, which is the address of the interface that connects to the WAN transport network (such as the Internet) or to the NAT gateway that connects to the WAN transport. Once the DTLS connection comes up between the Cisco vEdge router and Cisco SD-WAN Controller, OMP registers the TLOCs with Cisco SD-WAN Controller.
- The Cisco vEdge router advertises the IP addresses of any services that are located on its service-side network, such as firewalls and intrusion detection devices.

Cisco SD-WAN Controller installs these OMP routes in its routing database and advertises them to the other Cisco vEdge routers in the Cisco Catalyst SD-WAN overlay network. Cisco SD-WAN Controller also updates the Cisco vEdge router with the OMP route information that it learns from other Cisco vEdge routers in the network. Cisco SD-WAN Controller can apply inbound policy on received routes and prefixes before installing them into its routing table, and it can apply outbound policy before advertising routes from its routing table.

Firewall Ports for Cisco Catalyst SD-WAN Deployments

This article describes which ports Cisco Catalyst SD-WAN devices use. If your network has firewall devices, you must open these ports on the firewalls so that devices in the Cisco Catalyst SD-WAN overlay network can exchange traffic.

Cisco Catalyst SD-WAN-Specific Port Terminology

By default, all Cisco vEdge devices use base port 12346 for establishing the connections that handle control and traffic in the overlay network. Each device uses this port when establishing connections with other Cisco vEdge devices.



Note If a NAT gateway is present in the underlay and performs source port translation without preserving the original port, it may assign a random source port under certain conditions. This can occur when multiple devices are behind the same post-NAT IP address using the same source port, or if the port is already occupied by existing sessions. As a result, the assigned source port may differ from the specified range of UDP ports: 12346+n, 12366+n, 12386+n, 12406+n, and 12426+n, where n ranges from 0 to 19 and represents the configured offset. It is essential to consider this when configuring inbound firewall rules on the remote router's side.

Port Offset

When multiple Cisco vEdge devices are installed behind a single NAT device, you can configure different port numbers for each device so that the NAT can properly identify each individual device. You do this by configuring a port offset from the base port 12346. For example, if you configure a device with a port offset of 1, that device uses port 12347. The port offset can be a value from 0 through 19. The default port offset is 0.

For NAT devices that can differentiate among the devices behind the NAT, you do not need to configure the port offset.

Port Hopping

In the context of a Cisco Catalyst SD-WAN overlay network, port hopping is the process by which devices try different ports when attempting to establish connections with each other, in the event that a connection attempt on the first port fails. After such a failure, the port value is incremented and the connection attempt is retried. The software rotates though a total of five base ports, waiting longer and longer between each connection attempt.

If you have not configured a port offset, the default base port is 12346, and port hopping is done sequentially among ports 12346, 12366, 12386, 12406, and 12426, and then returning to port 12346.

If you have configured a port offset, that initial port value is used and the next port is incremented by 20. For example, for a port configured with an offset of 2, port hopping is done sequentially among ports 12348, 12368, 12388, 12408, and 12428, and then returning to port 12348.

Incrementing the ports by 20 ensures that there is never any overlap among the possible base port numbers.

Cisco vEdge devices use port hopping when attempting to establish connections to Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controllers. You can also manually request a Cisco vEdge device to port-hop.

Cisco SD-WAN Controllers and Cisco SD-WAN Manager instances are normally installed behind a properly behaving NAT device, so port hopping is generally not needed and generally does not occur on these devices.

Cisco SD-WAN Validators always connect to other Cisco vEdge devices using port 12346. They never use port hopping.

To describe how port hopping works, we use an example of a Cisco vEdge device with the default base port of 12346. When a router has attempted to connect to another Cisco vEdge device but the connection does not succeed within a certain time, the router hops to the next base port and tries establishing the connection on that port.

Note As port-hop is the default configuration, the devices request the Cisco SD-WAN Validator for a new control connection. When the new control connection is established, the edge devices start transmitting TLOC updates to the peer. TLOC update messages could be lost during unstable control connections and IPSec security association between the devices and the peer may not be in sync, which results in a BFD session failure.

To avoid this issue, we recommend that you configure no port-hop or static entries on data center devices. You can either have all edges connected to a single Cisco SD-WAN Validator or balance the edges between two Cisco SD-WAN Validators by changing the order of the IP in the below command.

For static entries, you can configure the IP addresses on a data center device in the following command:

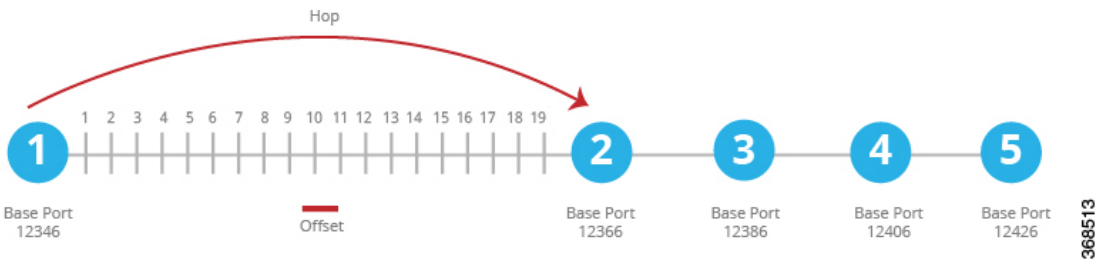
```
system
 vbond <vBond FQDN>
vpn 0
 host <vBond FQDN> ip <vBond ip1> <vBond ip2>
```

Note If you choose to configure no port-hopping, then use the following command:

```
system
 no port-hop
```

External triggers like change of System IP, change of Color on TLOC while adding TLOC can trigger port-hop, even though no port-hop is configured.

Figure 24: Example of Cisco vEdge Device Port Hopping



If the first connection attempt on the initial base port does not succeed after about 1 minute, the router hops to port 12366. After about 2 minutes, it hops to port 12386; after about 5 minutes, it hops to port 12406; and after about 6 minutes, it hops to port 12426. Then the cycle returns to initial port, 12346.

With a full-cone NAT device, the source ports for all connections initiated by a given Cisco vEdge device remain consistent across all sessions initiated by the Cisco vEdge device. For example, if the router initiates a session with public source port 12346, this is the port used for all communication.

Effects of Port Hopping

Cisco vEdge devices use port hopping to make every attempt to keep the control plane of the overlay network up and operational. If a controller device—Cisco SD-WAN Validator, Cisco SD-WAN Manager, or Cisco SD-WAN Controller—goes down for any reason and the Cisco vEdge devices remain up, when the controller device comes back up, the connection between it and the Cisco vEdge device might shut down and restart, and in some cases the BFD sessions on the Cisco vEdge device might shut down and restart. This behavior occurs because of port hopping: When one device loses its control connection to another device, it port hops to another port in an attempt to re-establish the connection.

Two examples illustrate when this might occur:

- When Cisco SD-WAN Validator crashes, Cisco SD-WAN Manager might take down all connections to the Cisco vEdge devices. The sequence of events that occurs is as follows: When Cisco SD-WAN Validator crashes, Cisco SD-WAN Manager might lose or close all its control connections. Cisco SD-WAN Manager then port hops, to try to establish connections to the Cisco SD-WAN Controllers on a different port. This port hopping on Cisco SD-WAN Manager shuts down and then restarts all its control connections, including those to the Cisco vEdge devices.
- All control sessions on all Cisco SD-WAN Controllers go down, and BFD sessions on the Cisco vEdge devices remain up. When any one of the Cisco SD-WAN Controllers comes back up, the BFD sessions on the routers go down and then come back up because the Cisco vEdge devices have already port hopped to a different port in an attempt to reconnect to Cisco SD-WAN Controllers.



Note Changing the Cisco SD-WAN Controller **graceful-restart timers** result in an OMP peer flap, independent of whether or not **port-hop** is enabled. We recommend that you change Cisco SD-WAN Controller **graceful-restart timers** with redundant Cisco SD-WAN Controller peering (where only a single Cisco SD-WAN Controller configuration is changed at a time) or during a maintenance period when a data plane disruption can be tolerated.

Ports Used by Cisco vEdge Devices

When a Cisco vEdge device joins the overlay network, it establishes DTLS control plane connections with the controller devices—Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller. The router uses these control connections to learn the location of Cisco Catalyst SD-WAN Controller from Cisco SD-WAN Validator, to receive its configuration from Cisco SD-WAN Manager, and to receive its policy and any policy updates from Cisco Catalyst SD-WAN Controller. When initially establishing these DTLS connections, the Cisco vEdge device uses the base port 12346. If it is unable to establish a connection using this base port, it port-hops through ports 12366, 12386, 12406, and 12426, returning, if necessary, to 12346, until it successfully establishes the DTLS connections with the three controller devices. This same port number is used to establish the IPsec connections and BFD sessions to the other Cisco vEdge devices in the overlay network. Note that if the vEdge configuration includes a port offset, the base port number and the four sequential port numbers are incremented by the configured offset.

To see which port DTLS and BFD are using for the control and data connections, look at the Private Port column in the output of the **show control local-properties** command. The command output also shows the

public port number that the interface is using. If the WAN port of the Cisco vEdge device is not connected to a NAT device, the private and public port numbers are the same. If a NAT device is present, the port number listed in the Public Port column is the one being used by the NAT device, and it is the port that BFD is using. This public port number is the one remote Cisco vEdge devices use to send traffic to the local site.

If a NAT device is present, the port number listed in the Public Port column is used by the NAT device, and BFD. This public port number is used by remote Cisco vEdge devices to send traffic to the local site.

In a network with firewall devices, you must open the Cisco Catalyst SD-WAN base ports on the firewall devices to allow traffic to flow across the overlay network. You open all the base ports that the Cisco vEdge devices in the network might use, which are the default base ports and the four base ports that the router can port-hop among.

Note Port hopping is generally not needed on Cisco SD-WAN Controllers and on Cisco SD-WAN Manager.

For additional details regarding DTLS, TLS, and IPsec ports for Cisco Catalyst SD-WAN device connections, see Firewall Port Considerations

For Cisco vEdge devices configured to use DTLS tunnels, which use UDP, at a minimum you must open the five base ports that are used by a Cisco vEdge device with a default port offset of 0. Specifically, you open:

- Port 12346
- Port 12366
- Port 12386
- Port 12406
- Port 12426

If you have configured a port offset value on any of the Cisco vEdge devices, you also need to open the ports configured with the port offset value:

- Port (12346 + port offset value)
- Port (12366 + port offset value)
- Port (12386 + port offset value)
- Port (12406 + port offset value)
- Port (12426 + port offset value)

Ports Used by Cisco Catalyst SD-WAN Devices Running Multiple vCPUs

The Cisco SD-WAN Controllers can run on a virtual machine (VM) with up to eight virtual CPUs (vCPUs). Cisco SD-WAN Manager can be configured to a minimum of 16 vCPUs, and eight vCPUs are used for control connection ports. The vCPUs are designated as Core0 through Core7.

Each core is allocated separate base ports for control connections. The base ports differ, depending on whether the connection is over a DTLS tunnel (which uses UDP) or a TLS tunnel (which uses TCP).

Note Cisco SD-WAN Validators do not support multiple cores. Cisco SD-WAN Validators always use DTLS tunnels to establish control connections with other Cisco vEdge devices, so they always use UDP. The UDP port is 12346.

The following table lists the port used by each vCPU core for Cisco SD-WAN Manager. Each port is incremented by the configured port offset, if offset is configured.

Core Number	Ports for DTLS (UDP)	Ports for TLS (TCP)
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

Administrative Ports Used by Cisco SD-WAN Manager

Cisco SD-WAN Manager uses the following administrative ports for protocol-specific communication:

Purpose	Traffic Direction	Protocol	Port Number
Netconf	Bidirectional Between Cisco SD-WAN Manager and Cisco SD-WAN Controllers or Cisco SD-WAN Validators.This port is used in Cisco SD-WAN Manager to establish initial discovery.	TCP	830 **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1, this port is accessible only via the Cisco IOS XE Catalyst SD-WAN device's system IP. Access to this port via other IP addresses is blocked.
HTTPS	Incoming	TCP	443
SNMP query	Incoming	UDP	161

Purpose	Traffic Direction	Protocol	Port Number
SSH	Incoming Cisco SD-WAN Manager uses SCP to install signed certificates onto the controllers if DTLS/TLS connections are not yet formed between them. SSH uses TCP destination port 22.	TCP	22
RADIUS	Outgoing	UDP	1812
SNMP trap	Outgoing	UDP	162
Syslog	Outgoing	UDP	514
TACACS	Outgoing	TCP	49

Cisco SD-WAN Manager clusters use the following ports for communication among the NMSs that comprise the cluster:

Cisco SD-WAN Manager Service	Traffic Direction	Protocol	Port Numbers
Application server	Bidirectional	TCP	80, 443, 7600, 8080, 8443, 57600
Configuration database	Bidirectional	TCP	5000, 7474, 7687
Coordination server	Bidirectional	TCP	2181, 2888, 3888
Message bus	Bidirectional	TCP	4222, 6222, 8222
Statistics database	Bidirectional	TCP	9200, 9300
Tracking of device configurations (NCS and Netconf)	Bidirectional	TCP	830
Cloud Agent	Bidirectional	TCP	8553
SD-AVC	Bidirectional	TCP	10502, 10503
Cloud Agent V2	Bidirectional	TCP	50051

Configure the Port Offset

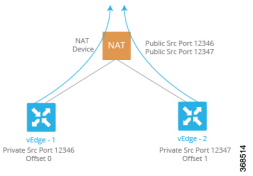
When two or more Cisco vEdge devices are behind the same full-cone NAT device, one device can use the default port offset, and you should configure a port offset on the remaining devices:

```
Device(config)# system port-offset number
```

The port offset can be a value from 0 through 19. The default port offset is 0.

In the following example, vEdge-1 uses the default port offset of 0, and on vEdge-2 the port offset is set to 1.

Figure 25: Example of Port Offset Configuration



In this example:

- vEdge-1 attempts to connect first using base port 12346. If that attempt is not successful, the router attempts port 12366, 12386, 12406 and 12426.
- vEdge-2 has a port offset of 1, so the first port it attempts to connect on is 12347 (12346 plus offset of 1). If it fails to connect using port 12347, the router hops by increments of 20 and attempts to connect on ports 12367, 12387, 12407, and 12427.

Perform Port Hopping Manually

You can manually request a Cisco vEdge device to port-hop:

```
vEdge# request port-hop
```

One reason to use this command is if the router's control connections are up, but BFD is not starting. The **request port-hop** command restarts the control connections on the next port number, and BFD should then also start.

Download Software

You can download Cisco Catalyst SD-WAN software from the Cisco Software Download site. The direct link for downloading Cisco Catalyst SD-WAN software is here.

Download the following components, and any other software that you need for your Cisco Catalyst SD-WAN installation. The Cisco SD-WAN Controllers operate as virtual machines on a server.

Note Starting from Cisco vManage Release 20.9.1, vEdge Cloud router is not supported.

Component	Comments
Cisco SD-WAN Validator	Appears as vEdge Cloud router on the download page because the Cisco SD-WAN Validator is deployed as a Cisco vEdge device.
Cisco SD-WAN Manager	Appears as Cisco SD-WAN Controller Software on the download page
Cisco Catalyst SD-WAN Controller	Appears as Cisco SD-WAN Controller Software on the download page

File Names for Cisco Catalyst SD-WAN Control Components Release 20.14.1 and Later

Starting from Cisco Catalyst SD-WAN Manager Release 20.14.1, the software images are renamed from viptela-edge to viptela-bond and an unified software image is used for Cisco SD-WAN Controller (vSmart)

and Cisco SD-WAN Validator (vBond). The initial default hostname for both controllers is vsmart. We recommend that you update the hostname.

Software Images	Before Cisco Catalyst SD-WAN Manager Release 20.14.1	Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later
.qcow2 (name change)	viptela-edge-genericx86-64.qcow2 viptela-image-generic86-64.qcow2	viptela-bond-genericx86-64.qcow2
.vhd (name change)	viptela-edge-genericx86-64_vhd.tar.gz viptela-image-generic86-64_vhd.tar.gz	viptela-bond-genericx86-64_vhd.tar.gz
.ova (name change)	viptela-edge-genericx86-64.ova viptela-image-generic86-64.ova	viptela-bond-genericx86-64.ova
.tar.gz (no change)	viptela-20.14.1-x86_64.tar.gz	viptela-20.14.1-x86_64.tar.gz

Deploy Cisco SD-WAN Manager

The Cisco SD-WAN Manager is a centralized network management system that provides a GUI interface to easily monitor, configure, and maintain all Cisco vEdge devices and links in the overlay network. The Cisco SD-WAN Manager runs as a virtual machine (VM) on a network server.

An SD-WAN overlay network can be managed by one Cisco SD-WAN Manager, or it can be managed by a cluster, which consists of a minimum of three Cisco SD-WAN Manager instances. It is recommended that you build a network, especially a larger network, with a Cisco SD-WAN Manager cluster. The Cisco SD-WAN Manager manages all the Cisco vEdge devices in the overlay network, providing dashboard and detailed views of device operation, and controlling device configurations and certificates.

Note Default route with non-zero prefix is not supported on vEdge routers.

To deploy Cisco SD-WAN Manager instances:

1. Create a Cisco SD-WAN Manager VM instance, either on an ESXi or a KVM hypervisor.
2. Create either a minimal or a full configuration for each of the Cisco SD-WAN Manager instance. You can configure Cisco SD-WAN Manager by using the ESXi console, or you can use SSH to open a CLI session and then manually configure Cisco SD-WAN Manager.
3. Configure certificate settings and generate a certificate for the Cisco SD-WAN Manager.
4. Create a Cisco SD-WAN Manager cluster.

Cisco SD-WAN Manager Web Server Ciphers

In Releases 16.3.0 and later, Cisco SD-WAN Manager web servers support the following ciphers:

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

In Release 16.2, Cisco SD-WAN Manager web servers support the following ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Create Cisco Catalyst SD-WAN Manager VM Instance on ESXi

Before You Begin

To run Cisco SD-WAN Manager, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This topic describes how to create a virtual machine on a server running the VMware vSphere ESXi Hypervisor. You can also create the virtual machine on a server running the Kernel-based Virtual Machine (KVM) hypervisor.

For server requirements, see Server Hardware Recommendations.

From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can enable disk encryption on the hypervisor.

Create Cisco Catalyst SD-WAN Manager VM Instance

1. Start the vSphere Client and create a Cisco SD-WAN Manager VM instance.
2. Create a new virtual disk that has a volume of at least 100 GB for the Cisco SD-WAN Manager database.
3. Add another vNICs.
4. Start the Cisco SD-WAN Manager VM instance and connect to the Cisco SD-WAN Manager console.
5. To create a Cisco SD-WAN Manager cluster, repeat Steps 1 through 4 to create a VM for each Cisco SD-WAN Manager instance.

If you are using the VMware vCenter Server to create the Cisco SD-WAN Manager VM instance, follow the same procedure.

Launch vSphere Client and Create Cisco Catalyst SD-WAN Manager VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the ESXi server, your username, and your password. Click **Login** to log in to the ESXi server.

   The system displays the ESXi screen.

2. Click **File** > **Deploy OVF Template** to deploy the virtual machine.
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vmanage.ova file that you downloaded from the Support page. Click **Next**.
4. Click **Next** to verify OVF template details.
5. Enter a name for the deployed template and click **Next**.
6. Click **Next** to accept the default format for the virtual disks.
7. From the **Destination Networks** drop-down list, select the destination network for the deployed OVF template, and click **Next**.
8. In the Ready to Complete screen, click **Finish** to complete deployment of the Cisco SD-WAN Manager VM instance.

The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

Create a New Virtual Disk

You must create a new virtual disk with a volume of at least 100 GB for the Cisco SD-WAN Manager database:

1. In the left navigation bar of the vSphere Client screen, select the Cisco SD-WAN Manager VM instance that you just created, and click **Edit** virtual machine settings.
2. In the Cisco SD-WAN Manager Virtual Machine Properties screen, click **Add** to add a new virtual disk, and then click **OK**.
3. In the Add Hardware screen, select **Hard Disk** for the device type you want to add to your VM, and click **Next**.
4. In the Select a Disk screen, select **Create a new virtual** disk, and click **Next**.
5. In the Create a Disk screen, specify the disk capacity for the Cisco SD-WAN Manager database to be 100 GB, and click **Next**.
6. In the Advanced Options screen, choose IDE (starting Cisco vManage Release 20.3.1, choose SCSI) for the virtual storage device, and click **Next**. If you are using IDE for release older than Cisco vManage Release 20.3.1, the virtual store device must be IDE.
7. In the Ready to Complete screen, click **Finish** to complete creating a new virtual disk with a capacity of 100 GB.

The system displays the vSphere Client screen with **Getting Started** selected.

Add Additional vNICs

To add another vNICs for the management interface and for the Message Bus:

1. In the left navigation bar of the vSphere Client, select the Cisco SD-WAN Manager VM instance that you just created, and click **Edit** virtual machine settings.
2. In the Cisco SD-WAN Manager – Virtual Machine Properties screen, click **Add** to add a new vNIC for the management interface. Then click **OK**.

3. Click Ethernet Adapter for the type of device you wish to add. Then click **Next**.
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.
5. In the Ready to Complete screen, click **Finish**.
6. The Cisco SD-WAN Manager – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.
7. If the Cisco SD-WAN Manager instance is part of a cluster, repeat Steps 2 through 6 to create a third vNIC. This vNIC is used for the Message Bus.

Connect Cisco Catalyst SD-WAN Manager VM Instance to Cisco Catalyst SD-WAN Manager Console

1. In the left navigation bar of the vSphere Client, select the Cisco SD-WAN Manager VM instance that you just created, and click **Power on the virtual machine**. The Cisco SD-WAN Manager virtual machine is powered on.
2. Select the **Console** tab, to connect to the Cisco SD-WAN Manager console. The Cisco SD-WAN Manager console is displayed. Log in to Cisco SD-WAN Manager.
3. Select the storage device to use.
4. Select **hdc**, which is the new partition you added for the Cisco SD-WAN Manager database.
5. Confirm that you want to format the new partition, **hdc**. The system then reboots and displays the Cisco SD-WAN Manager instance.
6. To connect to the Cisco SD-WAN Manager instance using a web browser, configure an IP address on the Cisco SD-WAN Manager instance:
   a. Log in to Cisco SD-WAN Manager.
   b. In the management VPN, VPN 512, configure an IP address on interface eth0. Specify an IP address that is reachable on your network. If necessary, add a default route:

```
# config
(config)# vpn 512
(config)# ip route prefix/length next-hop-ip-address
(config-vpn-512)# interface eth0
(config-interface-eth0)# ip address ip-address
(config-interface-eth0)# no shutdown
(config-interface-eth0)# commit and-quit
#
```

7. To connect to the Cisco SD-WAN Manager instance, type the following string in the URL:

   https:// *ip-address* **:8443/**

8. Log in.

   The default username and password is admin/admin.



Note Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, you can commit the configuration before rebooting a control manage device through Cisco SD-WAN Manager.

Create Cisco Catalyst SD-WAN Manager VM Instance on KVM

To run Cisco SD-WAN Manager, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This topic describes the process for creating a VM on a server running Kernel-based Virtual Machine (KVM) Hypervisor. You can also create the VM on a server running VMware vSphere ESXi Hypervisor.

For server requirements, see Server Hardware Requirements.

Create Cisco Catalyst SD-WAN Manager VM Instance on the KVM Hypervisor

To create a Cisco SD-WAN Manager VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager client application. The system displays the Virtual Machine Manager screen.
2. Click **New** to deploy the virtual machine. The Create a new virtual machine screen opens.
3. Enter the name of the virtual machine.
   a. Select **Import existing disk image** radio button.
   b. Click **Forward**. The virtual disk is imported and associated to the VM instance you are creating.
4. Provide the existing storage path box, click **Browse** to find the Cisco SD-WAN Manager software image.
   a. In the **OS Type** field, select **Linux**.
   b. In the **Version** field, select the Linux version that you are running.
   c. Click **Forward**.
5. Specify Memory and CPU based on your network topology and number of sites, and click **Forward**.
6. Select Customize configuration before install, and click **Finish**.
7. Select **Disk 1** in the left navigation bar.
   a. Click **Advanced Options**.
   b. In the Disk Bus field, choose IDE (staring Cisco vManage Release 20.3.1, choose SCSI).
   c. In the **Storage Format** field, choose **qcow2**.
   d. Click **Apply** to create the VM instance with the parameters you defined. By default, this VM instance includes one vNIC, which is used for the tunnel interface.

Note Cisco Catalyst SD-WAN supports only VMXNET3 vNICs.

8. In the Cisco SD-WAN Manager Virtual Machine window, click **Add Hardware** to add a new virtual disk for the Cisco SD-WAN Manager database.
9. In the Add New Virtual Hardware screen, specify the following for the new virtual disk:

a. In Create a disk image on the computer's hard drive, specify the disk capacity for the Cisco SD-WAN Manager database to be 100GB.

b. In the **Device Type** field, specify IDE disk (staring Cisco vManage Release 20.3.1, specify SCSI disk) for the virtual storage.

c. In the **Storage Format** field, specify **qcow2**.

d. Click **Finish** to complete the creation of a new virtual disk with a capacity of 100 GB.

10. In the Cisco SD-WAN Manager Virtual Machine screen, click **Add Hardware** to add another vNIC for the management interface.

11. In the Add New Virtual Hardware screen, click **Network**.

    a. In the **Host Device** field, select an appropriate host device.

    b. Click **Finish**.

    The newly created vNIC is listed in the left pane. This vNIC is used for the management interface.

12. If the Cisco SD-WAN Manager instance is a part of a cluster, repeat Steps 10 and 11 to create a third vNIC. This vNIC is used for the Message Bus.

13. In the Cisco SD-WAN Manager Virtual Machine screen click **Begin Installation** in the top upper-left corner of the screen.

14. The system creates the virtual machine instance and displays the Cisco SD-WAN Manager console.

15. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**. The system prompts you to select the storage device to use.

16. Select **hdc**, which is the new partition you added for the Cisco SD-WAN Manager database.

17. Confirm that you want to format the new partition, **hdc**. The system reboots and displays the Cisco SD-WAN Manager instance.

18. To create a Cisco SD-WAN Manager cluster, repeat Steps 1 through 17 to create a VM for each Cisco SD-WAN Manager instance.

Connect to a Cisco Catalyst SD-WAN Manager Instance

To connect to a Cisco SD-WAN Manager instance using a web browser, configure an IP address on the Cisco SD-WAN Manager instance:

1. Log in with the default username and password:

```
Login: admin password: admin #
```

2. In the management VPN, VPN 512, configure an IP address on interface eth0. Specify an IP address that is reachable on your network. If necessary, add a default route:

```
# config
(config)# vpn 512
(config)# ip route prefix/length next-hop-ip-address
(config-vpn-512)# interface  eth0
(config-interface-eth0)# ip address ip-address
(config-interface-eth0)# no shutdown
```

```
(config-interface-eth0)# command and-quit
#
```

3. To connect to the Cisco SD-WAN Manager instance, type the following string in the URL:

   https:// *ip-address* **:8443/**

4. Log in with the username **admin** and the password **admin**.

What to do next

From Cisco Catalyst SD-WAN Manager Release 20.18.1, for any new Cisco SD-WAN Manager deployments, when you first use Cisco SD-WAN Manager after onboarding, a guided task flow assists you through the essential configurations. See First Time Settings on Cisco SD-WAN Manager.

Configure Cisco Catalyst SD-WAN Manager

You can configure Cisco SD-WAN Manager using device templates. However, Cisco recommends that you use the CLI mode to configure Cisco SD-WAN Manager instead of using the device templates.

Once you have set up and started the virtual machines (VMs) for Cisco SD-WAN Manager, they come up with a factory-default configuration. You then configure each Cisco SD-WAN Manager instance directly from the Cisco SD-WAN Manager server itself using CLI mode or ESXi console so that each Cisco SD-WAN Manager can be authenticated and verified and can join the overlay network. At a minimum, you must configure the IP address of your network's Cisco SD-WAN Validator, the device's system IP address, and a tunnel interface in VPN 0 to use for exchanging control traffic among the network controller devices (the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controller devices).

For the overlay network to be operational and for Cisco SD-WAN Manager instances to participate in the overlay network, you must do the following:

- Configure a tunnel interface on at least one interface in VPN 0. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.
- Ensure that the Overlay Management Protocol (OMP) is enabled. OMP is the protocol responsible for establishing and maintaining the Cisco Catalyst SD-WAN control plane. OMP is enabled by default, and you cannot disable it. If you edit the configuration from the CLI, do not remove the **omp** configuration command.



Note For a Cisco SD-WAN Manager cluster, you must configure each Cisco SD-WAN Manager instance in the cluster individually, from the Cisco SD-WAN Manager server itself using CLI mode or ESXi console.

Configure Cisco Catalyst SD-WAN Manager

To configure Cisco SD-WAN Manager, create a device configuration template:

1. Configure the address of Cisco SD-WAN Validator:
   a. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
   b. Click **Validator**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.1 or earlier, click **Edit.**)

c. In the **Validator DNS/IP Address: Port** field, enter the DNS name that points to Cisco SD-WAN Validator or the IP address of Cisco SD-WAN Validator and the port number to use to connect to it.

d. Click **Save**.

2. Configure Cisco SD-WAN Manager Using CLI

   Use CLI mode to configure Cisco SD-WAN Manager. You can access the CLI by using the ESXi console using a separate SSH client or by establishing an SSH session through the Cisco SD-WAN Manager Graphical User Interface (GUI).

   To establish an SSH session to a device:

   a. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.

   b. From the left pane, click to select a device.

   c. Log in as the user admin, using the default password, admin. The CLI prompt is displayed.

   d. Enter configuration mode:

      Device# config

      Device(config)#

   You can now issue CLI commands to configure Cisco SD-WAN Manager.

   The following features are mandatory for Cisco SD-WAN Manager operation. Configure these features from the CLI mode.

   - Authentication, Authorization, and Accounting (AAA)
   - Security
   - System-wide parameters
   - Transport VPN (VPN 0)
   - Management VPN (for out-of-band management traffic)

Sample CLI Configuration

This section provides sample CLI configurations to configure Cisco SD-WAN Manager using CLI.

Note This configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vManage# show running-config
system
 host-name         vManage
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip         172.16.255.22
 site-id           200
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 vbond 10.1.14.14
```

```
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 !
 logging
  disk
   enable
  !
 !
!
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 community private
  view          v2
  authorization read-only
 !
 trap target vpn 0 10.0.1.1 16662
  group-name     Cisco
  community-name private
 !
 trap group test
  all
   level critical major minor
  exit
 exit
!
vpn 0
 interface eth1
  ip address 10.0.12.22/24
  tunnel-interface
   color public-internet
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0 10.0.12.13
!
vpn 512
 interface eth0
```

```
 ip 172.16.14.145/23
 no shutdown
!
ip route 0.0.0.0/0 172.16.14.1
!
```

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1, port 830, which is used for NETCONF, is closed by default. When the port is open, the configuration under the system-level hierarchy will show the **allow-service netconf** CLI command. If the port is closed, this command will either not appear in the configuration or will be displayed as **no allow-service netconf** within that same system-level hierarchy.

Configure Certificate Settings

New controller devices in the overlay network—Cisco SD-WAN Manager instances, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers—are authenticated using signed certificates. From Cisco SD-WAN Manager, you can automatically generate the certificate signing requests (CSRs), retrieve the generated certificates, and install them on all controller devices when they are added to the network.

Note All controller devices must have a certificate installed on them to be able to join the overlay network.

To automate the certificate generation and installation process, configure the name of your organization and certificate authorization settings before adding the controller devices to the network.

For more information on configuring certificate settings, see Certificates.

Generate Cisco Catalyst SD-WAN Manager Certificate

For Cisco SD-WAN Manager to be able to join the overlay network, you must generate a certificate signing request (CSR) for Cisco SD-WAN Manager instance. Cisco SD-WAN Manager automatically retrieves the generated certificate and installs it.

For more information on generating Cisco SD-WAN Manager certificate, see Certificates.

Create a Cisco Catalyst SD-WAN Manager Cluster

A Cisco SD-WAN Manager cluster is a collection of three or more Cisco SD-WAN Manager instances in a Cisco Catalyst SD-WAN overlay network domain. The cluster collectively provides network management services to all Cisco vEdge devices in the network. Some of the services, such as determining which Cisco SD-WAN Manager instance connects to and handles requests for a router, are distributed automatically, while for others (the statistics and configuration databases, and the messaging server), you configure which Cisco SD-WAN Manager instance handles the service.

For more information on creating Cisco SD-WAN Manager cluster, refer to Cluster Management.

Enable Timeout Value for a Cisco SD-WAN Manager Client Session

By default, a user's session to a Cisco SD-WAN Manager client remains established indefinitely and never times out.

To set how long a Cisco SD-WAN Manager client session is inactive before a user is logged out:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. Click **User Sessions**. In the **Client Session Timeout** option, enable the **Session Timeout**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.1 or earlier, click **Edit**.)
3. Enter the timeout value, in minutes. This value can be from 10 to 180 minutes.
4. Click **Save**.

The client session timeout value applies to all Cisco SD-WAN Manager servers in a Cisco SD-WAN Manager cluster.

Deploy Cisco Catalyst SD-WAN Validator

Cisco SD-WAN Validator is a software module that authenticates the Cisco SD-WAN Controllers and the vEdge routers in the overlay network and coordinates connectivity between them. It must have a public IP address so that all Cisco vEdge devices in the network can connect to it (it is the only Cisco vEdge device that must have a public address). While the Cisco SD-WAN Validator can be located anywhere in the network, it is strongly recommended that you place it in a DMZ. Assigning a public IP address to the orchestrator allows Cisco SD-WAN Controllers and vEdge routers that are situated in private address spaces, secured behind different NAT gateways, to establish communication connections with each other. Cisco SD-WAN Validator runs as a VM on a network server.

A Cisco Catalyst SD-WAN overlay network can have one or more Cisco SD-WAN Validators.

To deploy Cisco SD-WAN Validators:

1. Create a Cisco SD-WAN Validator VM instance, either on an ESXi or a KVM hypervisor.
2. Create a minimal configuration for Cisco SD-WAN Validator, to allow it to be accessible on the network. You do this by using SSH to open a CLI session to Cisco SD-WAN Validator and manually configuring the device.
3. Add Cisco SD-WAN Validator to the overlay network so that Cisco SD-WAN Manager is aware of it.
4. If you are hosting Cisco Catalyst SD-WAN zero-touch-provisioning (ZTP) Cisco SD-WAN Validator server in your enterprise, configure one Cisco SD-WAN Validator to perform this role.
5. Create a full configuration for Cisco SD-WAN Validator. You create the initial configuration by using SSH to open a CLI session to Cisco SD-WAN Validator. Then you create the full configuration by creating configuration templates on Cisco SD-WAN Manager and then attaching the templates to Cisco SD-WAN Validator. When you attach the configuration templates to Cisco SD-WAN Validator, the configuration parameters in the templates overwrite the initial configuration.

Create Cisco Catalyst SD-WAN Validator VM Instance on ESXi

Before You Begin

To start Cisco SD-WAN Validator, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the VMware vSphere ESXi Hypervisor. You can also create the VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software.

For server information, see Server Hardware Recommendations .

From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can enable disk encryption on the hypervisor.

Create Cisco Catalyst SD-WAN Validator VM Instance

1. Launch the vSphere client and create a Cisco SD-WAN Validator VM instance.
2. Add a vNIC for the tunnel interface.
3. Start the Cisco SD-WAN Validator VM instance and connect to the console.

The details of each step are provided below.

If you are using the VMware vCenter Server to create the Cisco SD-WAN Validator VM instance, follow the same procedure. Note, however, that the vCenter Server pages look different than the vSphere Client pages shown in the procedure.

Launch vSphere Client and Create a Cisco Catalyst SD-WAN Validator VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the EXSi server, your username, and your password. Click **Login** to log in to the ESXi server.
2. Click **File** > **Deploy OVF Template** to deploy the virtual machine.
3. In the Deploy OVF Template page, enter the location to install and download the OVF package. This package is the vedge.ova file that you downloaded from Cisco. Then click **Next**.
4. Click **Next** to verify OVF template details.
5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the Cisco SD-WAN Validator instance.
6. Click **Next** to accept the default format for the virtual disks.
7. Click **Next** to accept your destination network name as the destination network for the deployed OVF template. For this instance, CorpNet is the destination network.
8. In the Ready to Complete page, click **Finish**. The figure below shows the name for the Cisco SD-WAN Validator instance.

The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client page with **Getting Started** selected. By default, this includes one vNIC. This vNIC is used for the management interface.

Add a vNIC for the Tunnel Interface

1. In the left navigation bar of the vSphere Client, select the Cisco SD-WAN Validator VM instance you just created, and click **Edit virtual machine settings**.
2. In the vEdge Cloud – Virtual Machine Properties page, click **Add** to add a new vNIC for the management interface. Then click **OK**.
3. Click Ethernet Adapter for the type of device you wish to add. Then click **Next**.
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.
5. In the Ready to Complete page, click **Finish**.
6. The vEdge Cloud – Virtual Machine Properties page opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client page.

Start the Cisco Catalyst SD-WAN Validator VM Instance and Connect to the Console

1. In the left navigation bar of the vSphere Client, select the Cisco SD-WAN Validator virtual machine instance you created, and click **Power** on the virtual machine. The Cisco SD-WAN Validator virtual machine is powered on.
2. Select **Console** to connect to the Cisco SD-WAN Validator console.
3. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**.

What's Next

See *Configure Cisco Catalyst SD-WAN Validator*.

Create Cisco Catalyst SD-WAN Validator VM Instance on KVM

To start Cisco SD-WAN Validator, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor. You can also create the VM on a server running the vSphere ESXi Hypervisor software.

For server information, see *Server Hardware Recommendations*.

To create a Cisco SD-WAN Validator VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager page.
2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine page.
3. Enter the name of the virtual machine. The figure below specifies a name for the Cisco SD-WAN Validator instance.
   a. Choose **Import existing disk image** option to install the operating system.
   b. Click **Forward**.

4. For **Provide the existing storage path**, click **Browse** to find the Cisco SD-WAN Validator software image.
   a. For **OS Type**, choose **Linux**.
   b. For **Version**, choose the Linux version that you are running.
   c. Click **Forward**.
5. Specify Memory and CPU based on your network topology and the number of sites, and click **Forward**.
6. Check **Customize configuration before install**. Then click **Finish**.
7. Choose **Disk 1** in the left navigation bar. Then:
   a. Click **Advanced Options**.
   b. For **Disk Bus**, choose **IDE**.
   c. For **Storage Format**, choose **qcow2**.
   d. Click **Apply** to create the VM instance with the parameters you had defined. By default, this includes one vNIC. This vNIC is used for the management interface.

Note The software supports only VMXNET3 vNICs.

8. In the vEdge Cloud Virtual Machine page, click **Add Hardware** to add a second vNIC for the tunnel interface.
9. In the Add New Virtual Hardware page, click **Network**.
   a. In the **Host Device**, choose an appropriate **Host device**.
   b. Click **Finish**.

   The newly created vNIC is listed in the left pane. This vNIC is used for the tunnel interface.
10. In the Cisco SD-WAN Validator Virtual Machine page, click **Begin Installation** in the top upper-left corner of the page.
11. The system creates the virtual machine instance and displays the Cisco SD-WAN Validator console.
12. In the login page, log in with the default username, which is **admin**, and the default password, which is **admin**.

What's Next

See *Configure Cisco Catalyst SD-WAN Validator*.

Configure Cisco Catalyst SD-WAN Validator

Once you have set up and started the virtual machine (VM) for Cisco SD-WAN Validator in your overlay network, Cisco SD-WAN Validator comes up with a factory-default configuration. You then need to manually configure few basic features and functions so that the devices can be authenticated and verified and can join

the overlay network. Among these features, you configure the device as Cisco SD-WAN Validator providing the system IP address, and you configure a WAN interface that connects to the Internet. This interface must have a public IP address so that all Cisco vEdge devices in the overlay network can connect to Cisco SD-WAN Validator.

You create the initial configuration by using SSH to open a CLI session to Cisco SD-WAN Validator.

After you have created the initial configuration, you create the full configuration by creating configuration templates on Cisco SD-WAN Manager and then attach the templates to Cisco SD-WAN Validator. When you attach the configuration templates to Cisco SD-WAN Validator, the configuration parameters in the templates overwrite the initial configuration.

Create Initial Configuration for Cisco Catalyst SD-WAN Validator

To create the initial configuration on Cisco SD-WAN Validator using a CLI session:

1. Open a CLI session to Cisco vEdge device via SSH.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

   For Cisco Catalyst SD-WAN Control Components Release 20.14.x and later releases:

   ```
   vSmart# config
   vSmart(config)#
   ```

   For releases before Cisco Catalyst SD-WAN Control Components Release 20.14.x:

   ```
   vBond# config
   vBond(config)#
   ```

4. Configure the hostname:

   For Cisco Catalyst SD-WAN Control Components Release 20.14.x and later releases:

   ```
   vSmart(config)# system host-name vBond
   ```

   For releases before Cisco Catalyst SD-WAN Control Components Release 20.14.x:

   ```
   vBond(config)# system host-name hostname
   ```

   Configuring the hostname is optional, but is recommended because this name in included as part of the prompt in the CLI and it is used on various Cisco SD-WAN Manager screens to refer to the device.

5. Configure the system IP address:

   ```
   vBond(config-system)#system-ip ip-address
   ```

   Cisco SD-WAN Manager uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the IP address of Cisco SD-WAN Validator. Cisco SD-WAN Validator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach Cisco SD-WAN Validator:

   ```
   vBond(config-system)#vbond ip-address local
   ```

   In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. A Cisco SD-WAN Manager is effectively a vEdge router that performs only the orchestrator functions. The **local** option designates the device to be Cisco SD-WAN Validator, not a vEdge router. Cisco SD-WAN Validator must run on a standalone virtual machine (VM) or hardware router; it cannot coexist in the same device as a software or hardware vEdge router.

7. Configure a time limit for confirming that a software upgrade is successful:

   ```
   vBond(config-system)#upgrade-confirm minutes
   ```

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, Cisco SD-WAN Manager (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not received the confirmation within the configured time, it reverts to the previous software image.

8. Change the password for the user "admin":

   ```
   vBond(config-system)#user admin password password
   ```

   The default password is "admin".

9. Configure an interface in VPN 0, to connect to the Internet or other WAN transport network. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. Ensure that the prefix you configure for the interface contains the IP address that you configure in the **vbond local** command.

   ```
   vBond(config)#vpn 0 interface interface-name
   vBond(config-interface)#ip address ipv4-prefix/length
   vBond(config-interface)#ipv6 address ipv6-prefix/length
   vBond(config-interface)#tunnel-interface
   vBond(config-tunnel-interface)# encapsulation ipsec
   vBond(config-interface)#no shutdown
   ```

Note The encapsulation ipsec command is not mandatory for configuring a tunnel interface in these releases:

- Cisco Catalyst SD-WAN Control Components Release 20.18.1 and later
- Cisco Catalyst SD-WAN Control Components Release 20.15.3 and later release of 20.15.x

Note The IP address must be a public address so that all devices in the overlay network can reach Cisco SD-WAN Validator.

10. Commit the configuration:

    ```
    vBond(config)#commit and-quit
    vBond#
    ```

11. Verify that the configuration is correct and complete:

    ```
    vBond#show running-config
    ```

After the overlay network is up and operational, create a Cisco SD-WAN Validator configuration template on the Cisco SD-WAN Manager that contains the initial configuration parameters. Use the following Cisco SD-WAN Manager feature templates:

- System feature template to configure the hostname, system IP address, and Cisco SD-WAN Validator functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN Interface Ethernet feature template to configure the interface in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and configure Organization name.
- From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**. From System configuration template drop-down, select **create template** and configure Timezone, NTP servers, and device physical location.
- Click **Additional Templates** and from banner feature template drop-down, select **Create Template**. Configure Login banner.
- From System feature configuration template drop-down, select **Create Template** and configure disk and server parameters.
- From AAA feature configuration template drop-down, select **Create Template** and configure AAA, RADIUS and TACACS servers.
- Click **Additional Templates** and from SNMP feature template drop-down, select **Create Template** and configure SNMP.

Note For Cisco SD-WAN Validators, SNMP polling should only be performed using **vpn 512** interface.

Note The IP address must be a public address so that all devices in the overlay network can reach Cisco SD-WAN Validator.

Sample Initial CLI Configuration

Below is an example of a simple configuration on Cisco SD-WAN Validator. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vBond#show running-config
system
 host-name         vBond
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip         172.16.240.161
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 vbond 11.1.1.14 local
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
```

```
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 !
 logging
  disk
   enable
  !
!
vpn 0
 interface ge0/0
  ip address 11.1.1.14/24
  no shutdown
 !
 ip route 0.0.0.0/0 11.1.1.1
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

What's Next

See *Add Cisco SD-WAN Validator to the Overlay Network*.

Create Configuration Templates for Cisco Catalyst SD-WAN Validator

This article describes how to configure Cisco SD-WAN Validators that are being managed by Cisco SD-WAN Manager. These devices must be configured from Cisco SD-WAN Manager. If you configure them directly from the CLI on the router, Cisco SD-WAN Manager overwrites the configuration with the one stored on the NMS system.

Configuration Prerequisites

Security Prerequisites

Before you can configure Cisco SD-WAN Validators in the Cisco SD-WAN overlay network, you must have generated a certificate for Cisco SD-WAN Validator, and the certificate must already be installed on the device. See Generate a Certificate.

Variables Spreadsheet

The feature templates that you create will most likely contain variables. To have Cisco SD-WAN Manager populate the variables with actual values when you attach a device template to a device, either enter the values manually or click **Import File** in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in the order listed below):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).
- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network— routers, Cisco SD-WAN Controllers, and Cisco SD-WAN Validators. You do not need to specify values for all variables for all devices.

Feature Templates for Cisco Catalyst SD-WAN Validators

The following features are mandatory for Cisco SD-WAN Validator operation, and so creating a feature template for each of them is required:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN, with the VPN ID set to 0
Management VPN (for out-of-band management traffic)	VPN, with the VPN ID set to 512

Create Feature Templates

Feature templates are the building blocks of a Cisco SD-WAN Validator's complete configuration. For each feature that you can enable on Cisco SD-WAN Validator, Cisco SD-WAN Manager provides a template form that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco SD-WAN Validator features.

You can create multiple templates for the same feature.

To create Cisco SD-WAN Validator feature templates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select **Add Template**.
4. In the left pane, from **Select Devices**, select **Cloud router**.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters applicable to that template. Optional parameters are generally grayed out. A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.

6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu available to the left of each parameter's value box.
8. Click the plus sign (+) below the required parameters to set the values for additional parameters, if applicable.
9. Click **Create**.
10. Create feature templates for each of the required features listed in the previous section.
    a. In the System template, in the top portion, configure all desired parameters except for Controller Groups, Maximum Controllers, and Maximum OMP Sessions. These parameters are specific to routers and have no meaning for Cisco SD-WAN Validator. In the **Advanced Options** portion, in Cisco SD-WAN Validator Only and Local Cisco SD-WAN Validator, click **On**. These two parameters instantiates Cisco SD-WAN Validator.
    b. Create two VPN templates, one for VPN 0 (the VPN that connects to the Internet or other public transport network) and one for VPN 512 (the VPN that handles out-of-band management traffic).
    c. Create AAA and Security templates.
11. Create feature templates for each feature that you want to enable on Cisco SD-WAN Validators:
    a. Create Archive and Banner templates
    b. Create one Interface Ethernet template for each additional Ethernet interface you want to configure on the Cisco SD-WAN Validator. Cisco SD-WAN Validator needs tunnel interface configured in VPN 0. Refer to Changes in behavior in Release 20.18.1.

Create Device Templates

Device templates contain all or large portions of a device's complete operational configuration. You create device templates by consolidating together individual feature templates. You can also create them by entering a CLI text-style configuration directly on Cisco SD-WAN Manager. You can use both styles of device templates when configuring the Cisco SD-WAN Validator.

To create Cisco SD-WAN Validator device templates from feature templates:

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



Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down, select **From Feature Templates**.
4. From the **Device Model** drop-down, select a **Cloud router**.
5. Enter a name and description for the Cisco SD-WAN Validator device template. These fields are mandatory. You cannot use any special characters in template names.

6. From the **Load Running config from reachable device** drop-down, select the desired group of templates.
7. In each section, select the desired template. All required templates are marked with an asterisk (*). Initially, the drop-down for each template lists the default feature template.
   a. For each required and optional template, select the feature template from the drop-down. These templates are the ones that you previously created (see Create Feature Templates above). Do not select a BFD or an OMP template for Cisco SD-WAN Validators.
   b. For additional templates, click the plus (+) sign next to the template name, and select the feature template from the drop-down.
8. Click **Create**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

To create device templates by entering a CLI text-style configuration directly on Cisco SD-WAN Manager:

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



Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down, select **CLI Template**.
4. Enter a template name and description.
5. Enter the configuration in the **Config Preview** window, either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
7. Click **Add**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Attach Device Templates To Cisco Catalyst SD-WAN Validator

To configure Cisco SD-WAN Validator, you attach one device template to the orchestrator. You can attach the same template to multiple Cisco SD-WAN Validators simultaneously.

To attach a device template to the Cisco SD-WAN Validator:

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



Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. Select the desired device template.
4. For the selected device template, click **...**, and select **Attach Devices**.
5. In the **Attach Devices** column, select the desired Cisco SD-WAN Validator from the **Available Devices** list, and click the right-pointing arrow to move them to the **Selected Devices** column. You can select one or more orchestrators. Click **Select All** to choose all listed orchestrator.
6. Click **Attach**.

Add Cisco Catalyst SD-WAN Validator to the Overlay Network

After you create a minimal configuration for Cisco SD-WAN Validator, you must add it to overlay network by making Cisco SD-WAN Manager aware of Cisco SD-WAN Validator. When you add Cisco SD-WAN Validator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

Add Cisco Catalyst SD-WAN Validator and Generate Certificate

To add Cisco SD-WAN Validator to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Control Components** and click **Add Validator**.
3. In the **Add Validator** window:
   a. Enter the VPN 0 IP address.
   b. Enter the username and password to access Cisco SD-WAN Validator.
   c. Choose the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   d. Click **Add**.

Cisco SD-WAN Manager generates the CSR, retrieves the generated certificate, and automatically installs it on Cisco SD-WAN Validator. The new controller device is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on Cisco SD-WAN Validator:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose the new device listed, and check in the Certificate Status column to ensure that the certificate has been installed.

Start the Enterprise ZTP Server

The ZTP server must be configured before the ZTP workflow starts.

If you are hosting the Cisco Catalyst SD-WAN zero-touch-provisioning (ZTP) server in your enterprise, you must configure one Cisco SD-WAN Validator to perform this role. This Cisco SD-WAN Validator provides

the Cisco vEdge devices in the overlay network with the IP address of your enterprise Cisco SD-WAN Validator and with the enterprise root CA chain. You can think of this Cisco SD-WAN Validator server as a top-level Cisco SD-WAN Validator, analogous to a top-level domain server in the Internet.

If you are using the Cisco Catalyst SD-WAN ZTP hosted service, there is no need to set up a top-level Cisco SD-WAN Validator.

This section provides step-by-step instructions on how to start the Cisco SD-WAN Validator and perform initial configuration.

Requirements for ZTP

To start the Cisco SD-WAN Validator software, you need the following hardware and software components:

- A Cisco vEdge device on which the Cisco SD-WAN Validator software has been installed or the Cisco SD-WAN Validator VM instance on the hypervisor.
- Appropriate power cables. See the packing list for your hardware platform.
- An enterprise DNS server that has been configured with a record that redirects the URL ztp.cisco.com to your enterprise ZTP server. The recommended URL for this enterprise server is ztp.*local-domain*.
- Certificate generated as a result of a Certificate Signing Request (CSR).
- Enterprise root CA chain.
- For releases through Cisco SD-WAN Release 20.1.1 on Cisco vEdge devices, a CSV file that contains the Cisco vEdge device chassis information required by the Cisco SD-WAN Validator that is acting as the ZTP server. Each row in the CSV file must contain the following information for each Cisco vEdge device.



Note The ztp-server should be csr-cert signed from either cisco-pki or symantec (Digicert).



Note Some operating systems, including Microsoft Windows, may add carriage return special characters (such as ^M) at the end of each line in this file. Use a text editor to remove these characters before you upload the file.

  - vEdge router chassis number
  - vEdge router serial number
  - Validity (either valid or invalid)
  - Cisco SD-WAN Validator IP address
  - Cisco SD-WAN Validator port number (entering a value is optional)
  - Organization name as specified in the device certificate
  - Path to the enterprise root certification (entering a value is optional)

- For releases beginning with Cisco SD-WAN Release 20.3.1 on Cisco vEdge devices, a JSON file that contains the router chassis information that the Cisco SD-WAN Validator that acts as the ZTP server requires. This file is extracted from the PNP portal downloaded zip bundled device file. The JSON file contains the following information for each router:
  - Organization name as specified in the device certificate
  - Certificate information
  - Router chassis number
  - Router serial number
  - Validity (either valid or invalid)
  - Cisco SD-WAN Validator IP address
  - Cisco SD-WAN Validator port number (optional)



Note Before upgrading edge devices, ensure that your on-premises ZTP server is using the same release number (or higher) as the Cisco SD-WAN Controller release that you are using for Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator. For example, before upgrading from Cisco vManage Release 20.6.x to Cisco vManage Release 20.9.x, ensure that the ZTP server is using release 20.9 or later.

From Cisco SD-WAN Release 20.4.1, if **Multi-Tenancy** is enabled in controller profile on the PNP portal, the JSON file also contains the SP Organization Name.

For Cisco SD-WAN Release 20.3.1, download the Chassis ZIP file from the PNP portal and extract the JSON file from it. Use the following command to upload the JSON file to the ZTP server:

```
vBond# request device-upload chassis-file JSON-file-name
```

Here is an example of a JSON file:

```
{
              "version": "1.1",
              "organization": "vIPtela Inc Regression",
              "overlay": "vIPtela Inc Regression",
              "root_cert_bundle":"-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----",
              "controller_details": {
                    "primary_ipv4":"10.0.12.26",
                    "primary_port":"12346"
              },
              "chassis_list": [{
                     "chassis": "JAE214906FZ",
                     "SKU": "ASR1002-HX",
                     "HWPID": "ASR1002-HX",
                     "serial_list": [{
                                    "sudi_subject_serial": "JAE214906FX",
                                    "sudi_cert_serial": "021C0203",
                                    "HWPID": "ASR1002-HX"}]
                                    }
```

```
                                ],
                "timestamp": "2019-10-21 23:40:02.248"
}
```

From Cisco SD-WAN Release 20.3.2, you need not extract the JSON file from the Chassis ZIP file that you download from the PNP portal. Use the **request device-upload chassis-file** command to upload the `serialFile.Viptela` file downloaded from the PNP portal to the ZTP server. The ZTP server extracts the JSON file from `serialFile.Viptela` and loads the chassis entries into the database.

```
vBond# request device-upload chassis-file /home/admin/serialFile.viptela
Uploading chassis numbers via VPN 0
Copying ... /home/admin/serialFile.viptela via VPN 0
file:  /tmp/tmp.DkaQ18u3aM/viptela_serial_file
PnP
Verifying public key received from PnP against production root cert
is_public_key_ok against production root ca:  O = Cisco, CN = MMI Signer STG - DEV error
 20 at 0 depth lookup:unable to get local issuer certificate
Verifying public key received from PnP against engineering root cert
is_public_key_ok against engineering root ca:  OK
Signature verified for viptela_serial_file
final file:  /tmp/tmp.DkaQ18u3aM/viptela_serial_file
Removing unsigned file (cisco_cert.cer).
Signature verification Suceeded.
Success: Serial file is /tmp/tmp.DkaQ18u3aM/viptela_serial_file
INFO: Input File specified was '/usr/share/viptela/chassis_numbers.tmp'
INFO: Root Cert File is /home/admin/vIPtela Inc Regression.crt
INFO: # of complete chassis entries written: 19
Json to CSV conversion succeeded!
Successfully loaded the chassis numbers file to the database.
```

Optionally, you can configure the Cisco vEdge device information manually using the **request device** command.

Configure a Router to be a ZTP Server

To start the top-level Cisco SD-WAN Validator software and perform initial configuration:

1. Boot the Cisco vEdge device.
2. Use a console cable to connect a PC to the Cisco vEdge device.
3. Log in to the Cisco vEdge device using the default username, which is **admin**, and the default password, which is **admin**. The CLI prompt is displayed.
4. Configure the Cisco vEdge device to be a top-level Cisco SD-WAN Validator:

   ```
   vBond# config
   vBond(config)# system vbond ip-address local ztp-server
   ```

   The IP address must be a public address so that the Cisco SD-WAN Validator is reachable by all Cisco SD-WAN Controllers and Cisco vEdge devices through the transport network. The **local** option indicates that this Cisco vEdge device is acting as the Cisco SD-WAN Validator. It is this option that starts the Cisco SD-WAN Validator software process on the Cisco vEdge device. The **ztp-server** option establishes this Cisco SD-WAN Validator as the ZTP server.
5. Configure an IP address for the interface that connects to the transport network:

   ```
   vBond(config)# vpn 0 interface ge slot/port
   vBond(config-ge)# ip address prefix/length
   vBond(config-ge)# no shutdown
   ```
6. Commit the configuration:

```
vBond(config)# commit
```

7. Exit configuration mode:

```
vBond(config)# exit
```

8. Verify that the configuration is correct and complete:

```
vBond# show running-config
  system
   host-name               vm3
   system-ip               172.16.255.2
   admin-tech-on-failure
   route-consistency-check
   organization-name       "Cisco Inc"
   vbond 10.1.15.13 local ztp-server
```

9. Generate CSR manually:

```
vbond_ztp# request csr upload home/admin/vbond_ztp.csr
```

10. Sign CSR manually and generate certificate via PNP Connect Cisco PKI or Symantec via Cloud Ops.

11. Install Certificate:

```
vbond_ztp# request certificate install/home/admin/vbond_ztp.cer
```

12. Ensure Cisco IOS XE Catalyst SD-WAN has Cisco root-ca-cert or Symantec root-ca-cert in root-ca chain.

13. Check clock on vBond_ZTP and Cisco IOS XE Catalyst SD-WAN.

14. Upload the JSON file that contains the router chassis information to the ZTP server:

```
vBond# request device-upload chassis-file path
```

path is the path to a local file or a file on a remote device that is reachable via FTP, TFTP, HTTP, or SCP.

15. Verify that the list of Cisco vEdge device chassis numbers are present on the Cisco SD-WAN Validator using one of the following commands:

```
vBond# show ztp entries
vBond# show orchestrator valid-devices
```

Here is an example of the configuration of a top-level Cisco SD-WAN Validator:

```
vBond# show running-config vpn 0
interface ge0/0
  ip address 75.1.15.27/24
  !
  no shutdown
!

vBond# show running-config system
system
  vbond 75.1.15.27 local ztp-server
!
```

What's Next

See *Deploy the Cisco Catalyst SD-WAN Controller*.

vContainer Host

The support for vContainer Host is deferred. For more information on vContainer host, refer to deferral notice.

Deploy Cisco Catalyst SD-WAN Controller

Cisco SD-WAN Controller is the brains of the centralized control plane for the Cisco Catalyst SD-WAN overlay network, maintaining a centralized routing table and centralized routing policy. Once the network is operational, Cisco SD-WAN Controller effects its control by maintaining a direct DTLS control plane connection to each vEdge router. Cisco SD-WAN Controller runs as a virtual machine (VM) on a network server.

A Cisco Catalyst SD-WAN overlay network can have one or more Cisco SD-WAN Controllers. Cisco SD-WAN Controllers provide a means to control the flow of data traffic throughout the overlay network. It is recommended that an overlay network have at least two Cisco SD-WAN Controllers to provide redundancy. A single Cisco SD-WAN Controller can support up to 2,000 control sessions (that is, up to 2,000 TLOCs). Cisco SD-WAN Manager or Cisco SD-WAN Manager cluster can support up to 20 Cisco SD-WAN Controllers in the overlay network.

To deploy a Cisco SD-WAN Controller:

1. Create a Cisco SD-WAN Controller VM instance, either on an ESXi or a KVM hypervisor.
2. Create a minimal configuration for the Cisco SD-WAN Controller, to allow it to be accessible on the network. You do this by using SSH to open a CLI session to Cisco SD-WAN Controller and manually configuring the device.
3. Add Cisco SD-WAN Controller to the overlay network so that Cisco SD-WAN Manager is aware of it.
4. Create a full configuration for Cisco SD-WAN Controller. You do this by creating a Cisco SD-WAN Manager template for the Cisco SD-WAN Controller and attaching that template to the controller. When you attach the Cisco SD-WAN Manager template, the initial minimal configuration is overwritten.

Create Cisco Catalyst SD-WAN Controller VM Instance on ESXi

Before You Begin

To start the Cisco SD-WAN Controller, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the VMware vSphere ESXi Hypervisor software. You can also create the VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software.

For server requirements, see Server Hardware Recommendations.

From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can enable disk encryption on the hypervisor.

Create Cisco Catalyst SD-WAN Controller VM Instance

1. Launch the vSphere Client and create a Cisco SD-WAN Controller VM instance.

2. Add a vNIC for the management interface.
3. Start the Cisco SD-WAN Controller VM instance and connect to the console.

The details of each step are provided below.

If you are using the VMware vCenter Server to create the Cisco SD-WAN Controller VM instance, follow the same procedure. Note, however, that the vCenter Server pages look different than the vSphere Client pages shown in the procedure.

Launch vSphere Client and Create a Cisco Catalyst SD-WAN Controller VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the ESXi server, your username, and your password. Click **Login** to log in to the ESXi server.

   The system displays the ESXi screen.
2. Click **File** > **Deploy OVF Template** to deploy the virtual machine.
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vsmart.ova file that you downloaded from Cisco. Then click **Next**.
4. Click **Next** to verify OVF template details.
5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the Cisco SD-WAN Controller instance.
6. Click **Next** to accept the default format for the virtual disks.
7. Click **Next** to accept your destination network as the destination network for the deployed OVF template. In the figure below, CorpNet is the destination network.
8. In the Ready to Complete page, click **Finish**. The figure below shows the name for the Cisco SD-WAN Controller instance.

The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client page with **Getting Started** selected. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

Add a vNIC for the Management Interface

1. In the left navigation bar of the vSphere Client, select the Cisco SD-WAN Manager VM instance you just created, and click **Edit virtual machine settings**.
2. In the Cisco SD-WAN Manager – Virtual Machine Properties page, click **Add** to add a new vNIC for the management interface. Then click **OK**.
3. Click **Ethernet Adapter** for the type of device you wish to add. Then click **Next**.
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.
5. In the Ready to Complete page, click **Finish**.
6. The Cisco SD-WAN Manager – Virtual Machine Properties page opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client page.

Start the Cisco Catalyst SD-WAN Controller VM Instance and Connect to the Console

1. In the left navigation bar of the vSphere Client, select the virtual machine instance you just created, and click **Power on the virtual machine**. The Cisco SD-WAN Controller virtual machine is powered on.
2. Select **Console** to connect to the Cisco SD-WAN Controller console.
3. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**.

What's Next

See *Configure Cisco Catalyst SD-WAN Controller*.

Create Cisco Catalyst SD-WAN Controller VM Instance on KVM

To start the Cisco SD-WAN Controller, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software. You can also create the VM on a server running the VMware vSphere ESXi Hypervisor software.

For server requirements, see *Server Hardware Recommendations*.

To create a Cisco SD-WAN Controller VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager page.
2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine page.
3. Enter the name of the virtual machine. The figure below specifies a name for the Cisco SD-WAN Controller instance.
   a. Select **Import existing disk image**.
   b. Click **Forward**.
4. In **Provide the existing storage path** field, click **Browse** to find the Cisco SD-WAN Controller software image.
   a. For **OS Type**, select **Linux**.
   b. For **Version**, select the Linux version you are running.
   c. Click **Forward**.
5. Specify Memory and CPU based on your network topology and the number of sites, and click **Forward**.
6. Select Customize configuration before install. Then click **Finish**.
7. Select **Disk 1** in the left navigation bar. Then:
   a. Click **Advanced Options**.
   b. In the **Disk Bus** field, select **IDE**.
   c. In the **Storage Format** field, select qcow2.

d. Click **Apply** to create the VM instance with the parameters you just defined. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

Note The software supports only VMXNET3 vNICs.

8. In the Cisco SD-WAN Controller Virtual Machine page, click **Add Hardware** to add a second vNIC for the management interface.

9. In the Add New Virtual Hardware page, click **Network**.

a. In the **Host Device** field, select an appropriate host device.

b. Click **Finish**.

The newly created vNIC is listed in the left pane. This vNIC is used for the management interface.

10. In the Cisco SD-WAN Controller Virtual Machine page, click **Begin Installation** in the top upper-left corner of the screen.

11. The system creates the virtual machine instance and displays the Cisco SD-WAN Controller console.

12. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**.

What's Next

See *Configure Cisco Catalyst SD-WAN Controller*.

Configure the Cisco Catalyst SD-WAN Controller

Once you have set up and started the virtual machines (VMs) for the Cisco SD-WAN Controllers in your overlay network, they come up with a factory-default configuration. You then need to manually configure a few basic features and functions so that the devices can be authenticated and verified and can join the overlay network. These features include the IP address of your network's Cisco SD-WAN Validator, the device's system IP address, and a tunnel interface in VPN 0 to use for exchanging control traffic among the network controller devices (the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controller devices).

For the overlay network to be operational and for the Cisco SD-WAN Controllers to participate in the overlay network, do the following:

- Configure a tunnel interface on at least one interface in VPN 0. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.
- Ensure that the Overlay Management Protocol (OMP) is enabled. OMP is the protocol responsible for establishing and maintaining the Cisco Catalyst SD-WAN control plane. It is enabled by default, and you cannot disable it. When you edit the configuration from the CLI, do not remove the **omp** configuration command.

You create these initial configuration by using SSH to open a CLI session to the the Cisco SD-WAN Controller.

After you have created the initial configuration, you create the full configuration by creating configuration templates on the Cisco SD-WAN Manager NMS and then attaching them to the Cisco SD-WAN Controllers. When you attach the configuration template to the Cisco SD-WAN Controllers, the configuration parameters in the templates overwrite the initial configuration.

In this initial configuration, you should assign a system IP address to the Cisco SD-WAN Controller. This address, which is similar to the router ID on non-Cisco SD-WAN routers, is a persistent address that identifies the controller independently of any interface addresses. The system IP is a component of the device's TLOC address. Setting the system IP address for a device allows you to renumber interfaces as needed without affecting the reachability of the Cisco vEdge device. Control traffic over secure DTLS or TLS connections between Cisco SD-WAN Controllers and vEdge routers and between Cisco SD-WAN Controllers and Cisco SD-WAN Validator is sent over the system interface identified by the system IP address. In the transport VPN (VPN 0), the system IP address is used as the device's loopback address. You cannot use this same address for another interface in VPN 0.

Note For the overlay network to function properly and predictably, the policies configured on all Cisco SD-WAN Controllers must be identical.

Create Initial Configuration for the Cisco Catalyst SD-WAN Controller

To create the initial configuration on a Cisco SD-WAN Controller from a CLI session:

1. Open a CLI session to the Cisco vEdge device via SSH.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

   ```
   vSmart#  config
   vSmart(config)#
   ```

4. Configure the hostname:

   ```
   Cisco(config)# system host-name hostname
   ```

   Configuring the hostname is optional, but is recommended because this name in included as part of the prompt in the CLI and it is used on various Cisco SD-WAN Manager pages to refer to the device.

5. Configure the system IP address. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. Releases 19.1 and later do not allow the configuration of IPv6 unique local addresses. In these releases, configure IPv6 addresses from the FC00::/7 prefix range.

   Note Starting from Cisco Catalyst SD-WAN Control Components Release 20.9.x release, you can configure unique local IPv6 addresses. Prior to this release, you can configure IPv6 addresses from the FC00::/7 prefix range.

   ```
   vSmart(config-system)#system-ip ip-address
   ```

   The Cisco SD-WAN Manager uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the numeric identifier of the site where the device is located:

```
vSmart(config-system)# site-id site-id
```

7. Configure the numeric identifier of the domain in which the device is located:

   ```
   vSmart(config-system)# domain-id domain-id
   ```

8. Configure the IP address of the Cisco Catalyst SD-WAN Validator or a DNS name that points to the Cisco Catalyst SD-WAN Validator. The Cisco Catalyst SD-WAN Validator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach it.

   ```
   vSmart(config-system)# vbond  (dns-name | ip-address)
   ```

9. Configure a time limit for confirming that a software upgrade is successful:

   ```
   vSmart(config-system)# upgrade-confirm minutes
   ```

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, Cisco SD-WAN Manager (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not receive the confirmation within the configured time, it reverts to the previous software image.

10. Change the password for the user "admin":

    ```
    vSmart(config-system)# user admin password password
    ```

    The default password is "admin".

11. Configure an interface in VPN 0 to be used as a tunnel interface. VPN 0 is the WAN transport VPN, and the tunnel interface carries the control traffic among the devices in the overlay network. The interface name has the format **eth** *number*. You must enable the interface and configure its IP address, either as a static address or as a dynamically assigned address received from a DHCP server. In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address, or you can configure both to enable dual-stack operation. In earlier releases, it must be an IPv4 address.

    ```
    vSmart(config)# vpn 0
    vSmart(config-vpn-0)# interface interface-name
    vSmart(config-interface)# ( ip dhcp-client | ip address prefix/length)
    vSmart(config-interface)# (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [
    dhcp-distance number | dhcp-rapid-commit])
    vSmart(config-interface)# no shutdown
    vSmart(config-interface)# tunnel-interface
    vSmart(config-tunnel-interface)# allow-service netconf
    ```

Note You must configure a tunnel interface on at least one interface in VPN 0 in order for the overlay network to come up and for Cisco SD-WAN Controller to be able to participate in the overlay network. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

12. Configure a color for the tunnel to identify the type of WAN transport. You can use the default color (**default**), but you can also configure a more appropriate color, such as **mpls** or **metro-ethernet**, depending on the actual WAN transport.

    ```
    vSmart(config-tunnel-interface)# color color
    ```

13. Configure a default route to the WAN transport network:

    ```
    vSmart(config-vpn-0)# ip route 0.0.0.0/0 next-hop
    ```

14. Commit the configuration:

```
vSmart(config)# commit and-quit
vSmart#
```

15. Verify that the configuration is correct and complete:

```
vSmart# show running-config
```

After the overlay network is up and operational, create a Cisco SD-WAN Controller configuration template on the Cisco SD-WAN Manager that contains the initial configuration parameters. Use the following Cisco SD-WAN Manager feature templates:

- System feature template to configure the hostname, system IP address, and Cisco SD-WAN Validator functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN Interface Ethernet feature template to configure the interface, default route, and DNS server in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- From the Cisco SD-WAN Manager menu, select **Administration** > **Settings** and configure Organization name.
- From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates** and configure the following:
- For NTP and System feature configuration template, configure Timezone, NTP servers, and device physical location.

  Time Synchronize Cisco IOS XE Catalyst SD-WAN devices with Cisco SD-WAN Manager. Other wise, NTP issue occurs causing scheduled upgrade failure or certificate expiry.
- For Banner feature template, configure Login banner.
- For Logging feature configuration template, configure Logging parameters.
- For AAA feature configuration template, configure AAA, and RADIUS and TACACS+ servers.
- For SNMP feature configuration template, configure SNMP.

Sample Initial CLI Configuration

Below is an example of a simple configuration on a Cisco SD-WAN Controller. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vSmart# show running-config
system
 host-name         vSmart
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip         172.16.240.172
 site-id           200
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 upgrade-confirm   15
 vbond 184.122.2.2
 aaa
  auth-order local radius tacacs
  usergroup basic
```

```
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 !
 logging
  disk
   enable
  !
  server 192.168.48.11
   vpn      512
   priority warm
  exit
 !
!
omp
 no shutdown
 graceful-restart
!
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 community private
  view          v2
  authorization read-only
 !
 trap target vpn 0 10.0.1.1 16662
  group-name     Cisco
  community-name private
 !
 trap group test
  all
   level critical major minor
  exit
 exit
!
vpn 0
 interface eth1
  ip address 10.0.12.22/24
  tunnel-interface
   color public-internet
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service stun
 !
  no shutdown
 !
```

```
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

What's Next

See *Add the Cisco SD-WAN Controller to the Overlay Network*.

Create Configuration Templates for Cisco Catalyst SD-WAN Controller

For Cisco SD-WAN Controllers that are being managed by a Cisco SD-WAN Manager, you must configure them from Cisco SD-WAN Manager. If you configure them directly from the CLI on Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Manager overwrites the configuration with the one stored on Cisco SD-WAN Manager.

Configuration Prerequisites

Security Prerequisites

Before you can configure Cisco SD-WAN Controllers in the Cisco overlay network, you must have generated a certificate for Cisco SD-WAN Controller, and the certificate must already be installed on the device. See Generate a Certificate.

Variables Spreadsheet

The feature templates that you create will most likely contain variables. To have Cisco SD-WAN Manager populate the variables with actual values when you attach a device template to a device, either enter the values manually or click **Import File** in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in order):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).
- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network— routers, Cisco SD-WAN Controllers, and Cisco SD-WAN Validators. You do not need to specify values for all variables for all devices.

Feature Templates for Cisco Catalyst SD-WAN Controller

The following features are mandatory for Cisco SD-WAN Controller operation, so you must create a feature template for each of them:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Overlay Management Protocol (OMP)	OMP

Feature	Template Name
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN with the VPN ID set to 0
Management VPN (for out-of-band management traffic)	VPN with the VPN ID set to 512

Create Feature Templates

Feature templates are the building blocks of Cisco SD-WAN Controller's complete configuration. For each feature that you can enable on Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Manager provides a template form that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco SD-WAN Controller features.

You can create multiple templates for the same feature.

To create Cisco SD-WAN Controller feature templates:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates**.
2. Click **Feature Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Select **Add Template**.
4. In the left pane, from **Select Devices**, select **Controller**. You can create a single feature template for features that are available on both Cisco SD-WAN Controllers and other devices. You must, however, create separate feature templates for software features that are available only on Cisco SD-WAN Controllers.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining parameters applicable to that template. Optional parameters are generally grayed out. A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter field.
8. Click the plus sign (+) below the required parameters to set values for additional parameters, if applicable.
9. Click **Create**.
10. Create feature templates for each of the required features listed in the previous section. For the transport VPN, use the template called VPN-vSmart and in the VPN Template section, set the VPN to 0, with a scope of Global. For the management VPN, use the template called VPN- and in the VPN Template section, set the VPN to 512, with a scope of Global.

11. Create any additional feature templates for each optional feature that you want to enable on Cisco SD-WAN Controllers.

Create Device Templates

Device templates contain a device's complete operational configuration. You create device templates by consolidating together individual feature templates. You can also create them by entering a CLI text-style configuration directly on Cisco SD-WAN Manager.

You can attach only one device template to configure a Cisco SD-WAN Controller, so it must contain, at a minimum, all the required portions of the Cisco SD-WAN Controller configuration. If it does not, the Cisco SD-WAN Manager returns an error message. If you attach a second device template to the Cisco SD-WAN Controller, it overwrites the first one.

To create device templates from feature templates:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates**.
2. Click **Device Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down select **From Feature Templates**.
4. From the **Device Model** drop-down list, select **Controller**.
5. Enter a name and description for the Cisco SD-WAN Controller device template. These fields are mandatory. You cannot use any special characters in template names.
6. Complete the **Required Templates** section. All required templates are marked with an asterisk.
   a. For each required template, select the feature template from the drop-down list. These templates are the ones that you previously created (see Create Feature Templates above). After you select a template, the circle next to the template name turns green and displays a green check mark.
   b. For templates that have Sub-Templates, click the plus (+) sign or the Sub-Templates title to display a list of sub-templates. As you select a sub-template, the name of the sub-template along with a drop-down is displayed. If the sub-template is mandatory, its name is marked with an asterisk.
   c. Select the desired sub-template.
7. Complete the **Optional Templates** section, if required. To do so:
   a. Click **Optional Templates** to add optional feature templates to the device template.
   b. Select the template to add.
   c. Click the template name and select a specific feature template.
8. Click **Create**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

To create device templates by entering a CLI text-style configuration directly on Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, select **CLI Template**.
4. In the **Add Device CLI Template** window, enter a template name and description, and select **Controller**.
5. Enter the configuration in the **CLI Configuration** box, either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
7. Click **Add**. The right pane on the screen lists the new device template. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Attach a Device Template To Cisco SD-WAN Controllers

To configure a Cisco SD-WAN Controller, you attach one device template to the controller. You can attach the same template to multiple Cisco SD-WAN Controller simultaneously.

To attach a device template to Cisco SD-WAN Controllers:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. For the desired device template, click **...**, and select **Attach Devices**.
4. In the **Attach Devices** window, select the desired Cisco SD-WAN Controller from the **Available Devices** column, and click the right-pointing arrow to move them to the **Selected Devices** column. You can select one or more controllers. Click **Select All** to choose all listed controllers.
5. Click **Attach**.
6. Click **Next**.
7. To preview the configuration that is about to be sent to Cisco SD-WAN Controller, in the left pane, click the device. The configuration is displayed in the right pane, in the **Device Configuration Preview** window.
8. To send the configuration in the device template to Cisco SD-WAN Controllers, click **Configure Devices**.

Add Cisco Catalyst SD-WAN Controller to the Overlay Network

After you create a minimal configuration for Cisco SD-WAN Controller, you must add it to an overlay network by making Cisco SD-WAN Manager aware of the controller. When you add Cisco SD-WAN Controller, a signed certificate is generated and is used to validate and authenticate the controller.

Cisco SD-WAN Manager can support up to 20 Cisco SD-WAN Controllers in the network.

Add a Cisco Catalyst SD-WAN Controller and Generate Certificate

To add a Cisco SD-WAN Controller to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and from the **Add Controller** drop-down menu.

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.

3. In the **Add Controller** window:
   a. Enter the system IP address of Cisco SD-WAN Controller.
   b. Enter the username and password to access Cisco SD-WAN Controller.
   c. Choose the protocol to use for control-plane connections. The default is DTLS.
   d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   e. Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   f. Click **Add**.

Cisco SD-WAN Manager automatically generates the CSR, retrieves the generated certificate, and installs it on Cisco SD-WAN Controller. The new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on a Cisco SD-WAN Controller:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose the new controller listed and check in the Certificate Status column to ensure that the certificate has been installed.

Note If Cisco SD-WAN Controller and Cisco SD-WAN Validator have the same system IP addresses, they do not appear in Cisco SD-WAN Manager as devices or controllers. The certificate status of Cisco SD-WAN Controller and Cisco SD-WAN Validator is also not displayed. However, the control connections still successfully comes up.

What's Next

See *Deploy the vEdge Routers*.

Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals

Table 25: Feature History

Feature Name	Release Information	Description
Support for Deploying Cisco Catalyst 8000V Instances for Supported Cloud Services Provider Platforms	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Starting from this release, Cisco Catalyst 8000V instances can be deployed on Cloud Services Provider portals such as Google Cloud Platform, Microsoft Azure and Amazon Web Services.
Support for Deploying Cisco Catalyst 8000V Instances on Alibaba Cloud	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Starting from this release, Cisco Catalyst 8000V instances can be deployed on Alibaba Cloud.

For information on supported instances of Cisco Catalyst 8000V and how to deploy them on the supported cloud service provider portals, see the following links:

- Deploying Cisco Catalyst 8000V Edge Software on Amazon Web Services
- Deploying Cisco Catalyst 8000V Edge Software on Microsoft Azure
- Deploying Cisco Catalyst 8000V Edge Software on Google Cloud Platform
- Cisco Catalyst 8000V Edge Software Deployment Guide for Alibaba Cloud

Notes and Limitations

- Creating new Cisco Catalyst 8000V instances by snapshot: Creating a new Cisco Catalyst 8000V instance by snapshot (cloning) results in a new instance with the same serial number as the original. This creates a conflict in Cisco Catalyst SD-WAN. You can use the snapshot (cloning) function to create a new instance only if the new instance is replacing an existing one, so that the serial number will be used with only one Cisco Catalyst 8000V instance.

Deploy Cisco CSR 1000v Using Cloud Service Provider Portals

For information on supported instances of Cisco CSR 1000v routers and how to deploy them on the supported cloud service provider portals, see the following links:

- Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services
- Cisco CSR 1000v Deployment Guide for Microsoft Azure

Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud

This section provides information helpful when using the Alibaba Cloud instance with Cisco Catalyst SD-WAN. For detailed information about the Cisco Catalyst 8000V Edge Software deployment process, see Cisco Catalyst 8000V Edge Software Deployment Guide for Alibaba Cloud.

Features

The following Cisco Catalyst 8000V features are not supported in an Alibaba Cloud deployment when operating as part of Cisco Catalyst SD-WAN:

Table 26: Unsupported Features

Feature	Additional Information
Deployment and Licensing	
Cisco Catalyst SD-WAN Cloud onRamp integration	Connect the Cisco Catalyst 8000V to Cisco Catalyst SD-WAN by creating a bootstrap file, as described in Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco Catalyst SD-WAN, on page 201. Deployment by Cloud onRamp is not supported.
Pay as you go (PAYG) licensing	None

Requirements for the Cisco Catalyst 8000V Instance

The Cisco Catalyst 8000V instance deployed in Alibaba Cloud must meet the following requirements to work with Cisco Catalyst SD-WAN:

- Alibaba Cloud Elastic Compute Service (ECS) instance type: G5ne
- vCPU: 2
- RAM: 8 GB

The following image options are supported by Cisco Catalyst SD-WAN:

- ecs.g5ne.large: 2 vCPU and 8 GB RAM
- ecs.g5ne.xlarge: 4 vCPU and 16 GB RAM
- ecs.g5ne.2xlarge: 8 vCPU and 32 GB RAM

Configure the Cisco Catalyst 8000V Instance to Connect to Cisco Catalyst SD-WAN

When you create a Cisco Catalyst SD-WAN instance on Alibaba Cloud, create a Day 0 bootstrap file using Cisco SD-WAN Manager and use this bootstrap file on the Cisco Catalyst 8000V instance to onboard the

instance to Cisco Catalyst SD-WAN. When the instance starts up using the bootstrap file, it connects to the Cisco SD-WAN Validator and Cisco SD-WAN Manager controller.

Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco Catalyst SD-WAN

1. For instructions on creating a bootstrap file for a cloud-hosted device, using Cisco SD-WAN Manager, see Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices.
2. In the Alibaba Cloud portal, create an instance of the Cisco Catalyst 8000V. When configuring the instance, use the bootstrap configuration that you created in Cisco SD-WAN Manager.

Deploy the vEdge Cloud routers

vEdge routers, as their name implies, are edge routers that are located at the perimeters of the sites in your overlay network, such as remote office, branches, campuses, and data centers. They route the data traffic to and from their site, across the overlay network.

vEdge routers are either physical hardware routers or software vEdge Cloud router, which run as virtual machines on a hypervisor or an AWS server.

An overlay network can consist of a few or a large number of vEdge routers. A singleCisco SD-WAN Manager, which provides management and configuration services to the vEdge routers, can support up to about 2,000 routers, and a Cisco SD-WAN Manager cluster can support up to about 6,000 routers.

To deploy vEdge Cloud routers:

1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor.
2. For software vEdge Cloud router, install a signed certificate on the router. In Releases 17.1 and later, Cisco SD-WAN Manager can act as a Certificate Authority (CA) and can automatically generate and installed signed certificates on vEdge Cloud router. In earlier releases, send a certificate signing request to Symantec and then install that certificate on the router so that the router can be authenticated on and can participate in the overlay network.
3. From Cisco SD-WAN Manager, send the serial numbers of all vEdge Cloud routers to Cisco SD-WAN Controllers and Cisco SD-WAN Validators in the overlay network.
4. Create a full configuration for the vEdge Cloud router. You do this by creating a Cisco SD-WAN Manager template for Cisco SD-WAN Validator and attaching that template to the orchestrator. When you attach the Cisco SD-WAN Manager template, the initial minimal configuration is overwritten.
5. Prepare hardware vEdge Cloud router for automatic provisioning , which is done using the Cisco Catalyst SD-WAN zero-touch provisioning (ZTP) tool. The ZTP process allows hardware routers to join the overlay network automatically.

Starting with Release 18.2.0, vEdge Cloud routers that are hosted in countries affected by United States government embargoes cannot connect to overlay network controllers (Cisco SD-WAN Validators, Cisco SD-WAN Managers, and Cisco SD-WAN Controllers) that are hosted in the Cisco cloud. Any vEdge Cloud router from an embargoed country that attempts to connect to one of these controllers will be disabled. (The vEdge Cloud routers can, however, connect to controllers that are hosted in other clouds). As a result, when

a vEdge Cloud router initially attempts to connect to a controller in the Cisco cloud, the router might not come up and might remain in a pending state if the Cisco SD-WAN Validator and theCisco SD-WAN Manager are unable to communicate with each other or if the Cisco cloud server is down.

Create vEdge Cloud router VM Instance on AWS



Note Starting from Cisco vManage Release 20.9.1, vEdge Cloud router is not supported.

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on Amazon AWS. You can also create the VM on a server running the vSphere ESXi Hypervisor software or the Kernel-based Virtual Machine (KVM) Hypervisor software.

To start the vEdge Cloud router virtual machine (VM) instance on Amazon AWS, first create a Virtual Private Cloud (VPC). The VPC is a self-contained environment in which you build the infrastructure you need in order to build your network.

Plan your network addressing carefully before creating the VPC. The VPC can use addresses only in the range you specify, and once you create a VPC, you cannot modify it. If your network addressing requirements change, you must delete the VPC and create a new one.

Starting Cisco SD-WAN 18.4 Release, Cisco Cloud Services 1000v (CSR 1000v) Router Cisco Catalyst SD-WAN version is supported on AWS.

To start a vEdge Cloud router on Amazon AWS:

1. Create a VPC.
2. Set up the vEdge Cloud router VM instance.
3. Define additional interfaces.

Create a VPC

Plan your network address blocks carefully before creating the VPC. Once you create a VPC, you cannot modify it. To make any changes to the network addressing, you must delete the VPC and create a new one.

1. Log in to AWS. In the Networking section of the AWS home page, click **VPC**.
2. On the page that opens, click **Start VPC**.
3. On the Select a VPC Configuration page, select **VPC with Public and Private Subnets**.
4. On the VPC with Public and Private Subnets screen:
   a. In IP CIDR Block, enter the desired IP addressing block. The VPC can use addresses only in this ange.
   b. Specify a public subnet and a private subnet from within the IP CIDR block.
   c. In Elastic IP Allocation ID, enter the address of your Internet gateway. This gateway translates internal traffic for delivery to the public Internet.
   d. Add endpoints for S3 only if you need extended storage space, such as for a large database.
   e. To use the AWS automatic registration of IP addresses to DNS, enable DNS hostnames.

f. Select the desired Hardware tenancy, either shared or dedicated. You can share your AWS hardware with other AWS clients, or you can have dedicated hardware. With dedicated hardware, the device assigned to you can host only your data. However, the cost is higher.

g. Click **Create VPC**.

Wait a few minutes until the VPC Dashboard displays the VPC Successfully Created message.

The infrastructure is now complete and ready for you to deploy applications, appliances, and the vEdge Cloud router. Click the links on the left to see the subnets, route tables, internet gateways, and NAT address translation points in the VPC.

Set Up the vEdge Cloud router VM Instance

1. Click **Services** > **EC2** to open the EC2 Dashboard, and then click **Launch Instance**.

1. Choose an Amazon Machine Image (AMI). The Cisco Catalyst SD-WAN AMI has a name in the format *release-number*-vEdge; for example, 16.1.0-vEdge. The Cisco Catalyst SD-WAN AMI is private. Contact your Cisco Catalyst SD-WAN sales representative, who can share it with you.
2. Choose the Cisco Catalyst SD-WAN AMI, then click **Select**.
3. The Choose an Instance Type screen appears. Determine which instance type best meets your needs, according to the following table. The minimum requirement is 2 vCPUs.

Table 27: Table 1: EC2 Instance Types that Support the vEdge Cloud router

	vCPU	Memory (GB)	Instance Storage (GB)
General Purpose — Current Generation			
m4.large	2	8	EBS only
m4.xlarge	4	16	EBS only
m4.2xlarge	8	32	EBS only
m4.4xlarge	16	64	EBS only
m4.10xlarge	40	160	EBS only
Compute Optimized — Current Generation			
c4.large	2	3.75	EBS only
c4.xlarge	4	7.5	EBS only
c4.2xlarge	8	15	EBS only
c4.4xlarge	16	30	EBS only
c4.8xlarge	36	60	EBS only
c3.large	2	3.75	2 x 16 SSD

	vCPU	Memory (GB)	Instance Storage (GB)
c3.xlarge	4	7.5	2 x 40 SSD
c3.2xlarge	8	15	2 x 80 SSD
c3.4xlarge	16	30	2 x 160 SSD
c3.8xlarge	32	60	2 x 320 SSD

4. Select the preferred instance type, then click **Next**: Configure Instance Details.

Configure Instance Details

On the Configure Instance Details screen:

1. In Network, select the VPC you just created.
2. In Subnet, select the subnet for your first interface.
3. In Network Interfaces, click **Add Device** and select a subnet for each additional interface.

Note Starting from Cisco SD-WAN Release 20.5.1, a Cisco vEdge Cloud router VM with the default username and password (admin/admin) cannot be deployed on AWS. Therefore, when you deploy a Cisco vEdge Cloud router VM using a third-party cloud provider, ensure that you use the following cloud configuration to continue using the default credentials.

In the **User Data** field, enter the following cloud configuration:

```
#cloud-config

hostname: vedge
write_files:
- content: "vedge\n"
  owner: root:root
  path: /etc/default/personality
  permissions: '0644'
- content: "1\n"
  owner: root:root
  path: /etc/default/inited
  permissions: '0600'
- path: /etc/confd/init/zcloud.xml
  content: |
    <config xmlns="http://tail-f.com/ns/config/1.0">
      <system xmlns="http://viptela.com/system">
        <aaa>
          <user>
            <name>admin</name>

<password>$6$9ac6af765f1cd0c0$jRM/rCPsQ56J1DU/1s9H7zhhksy/FZHv37zDJkzM6h/IU/FsrITcBuLwV3AVI5kCnfX9wYmqP8CsGk.4PrjC22/</password>

            <group>netadmin</group>
          </user>
        </aaa>
      </system>
    </config>
```

This cloud configuration configures the VM with admin/admin credentials, and forces a password change on your first login.

5. Click **Next: Add Storage**.
6. The Add Storage page opens. You do not need to change any settings on this screen. Click **Next: Tag Instance**.
7. The Tag Instance page opens. Enter your desired Key and Value, and then click **Next: Configure Security Group**.
8. The Configure Security Group page opens. Add rules to configure your firewall settings. These rules apply to outside traffic coming into your vEdge Cloud router.
   a. Below **Type**, select **SSH**.
   b. Below **Source**, select **My IP**.
9. Click **Add Rule**, then fill out the fields as follows:
   a. Below **Type**, select **Custom UDP Rule**.
   b. Below **Port Range**, enter **12346**.
   c. Below **Source**, select **Anywhere**. 12346 is the default port for IPSec.
   d. If **port hopping** is enabled, you may need to add more rules.
10. Click **Review and Launch**. The Review Instance Launch screen opens. Click **Launch**.
11. Select **Proceed without a key pair**, click the acknowledgement check box, then click **Launch Instances**.
12. Wait a few minutes, the instance initializes. The vEdge Cloud router is now running. The first interface, eth0, is always the management interface. The second interface, ge0/0, appears in VPN 0, but you can configure it to be in a different VPN.

Define Additional Interfaces

The vEdge Cloud router supports a total of nine interfaces. The first is always the management interface, and the remaining eight are transport and service interfaces. To configure additional interfaces:

1. In the left pane, click **Network Interfaces**.
2. Click **Create Network Interface**. Select the **Subnet and Security group**, and then click **Yes, Create**. Note that two interfaces in the same routing domain cannot be in the same subnet.
3. Select the check box to the left of the new interface, and click **Attach**.
4. Select the vEdge Cloud router, and click **Attach**.
5. Reboot the vEdge Cloud router, because the vEdge Cloud router detects interfaces only during the boot process.

   The new interface is now up. The interface in VPN 0 connects to a WAN transport, such as the internet. The interface in VPN 1 faces a service-side network and can be used for appliances and applications. The interface in VPN 512 is dedicated to out-of-band management.

6. To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU from the CLI. For example:

```
Router# show interface
                                        IF      IF
                            TCP
                 AF                     ADMIN   OPER    ENCAP
              SPEED          MSS                RX      TX
VPN  INTERFACE  TYPE  IP ADDRESS        STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR
              MBPS   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------------
0    ge0/0      ipv4  10.66.15.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:62  1000   full    1420    0:14:05:07  545682   545226
0    ge0/1      ipv4  10.1.17.15/24     Up      Up      null   service    1500
00:0c:29:db:f0:6c  1000   full    1420    0:14:21:19  0        10
0    ge0/2      ipv4  -                 Down    Up      null   service    1500
00:0c:29:db:f0:76  1000   full    1420    0:14:21:47  0        0
0    ge0/3      ipv4  10.0.20.15/24     Up      Up      null   service    1500
00:0c:29:db:f0:80  1000   full    1420    0:14:21:19  0        10
0    ge0/6      ipv4  172.17.1.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:9e  1000   full    1420    0:14:21:19  0        10
0    ge0/7      ipv4  10.0.100.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:a8  1000   full    1420    0:14:21:19  770      705
0    system     ipv4  172.16.255.15/32  Up      Up      null   loopback   1500
00:00:00:00:00:00  0      full    1420    0:14:21:30  0        0
0    loopback3  ipv4  10.1.15.15/24     Up      Up      null   transport  2000
00:00:00:00:00:00  10     full    1920    0:14:21:22  0        0
1    ge0/4      ipv4  10.20.24.15/24    Up      Up      null   service    2000
00:0c:29:db:f0:8a  1000   full    1920    0:14:21:15  52014    52055
1    ge0/5      ipv4  172.16.1.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:94  1000   full    1420    0:14:21:15  0        8
512  eth0       ipv4  10.0.1.15/24      Up      Up      null   service    1500
00:50:56:00:01:05  0      full    0       0:14:21:16  28826    29599

Router# config
Entering configuration mode terminal
Router(config)# vpn 0 interface ge0/3 mtu 2000
Router(config-interface-ge0/3)# commit
Commit complete.
vEdge(config-interface-ge0/3)# end
vEdge# show interface
                                        IF      IF
                            TCP
                 AF                     ADMIN   OPER    ENCAP
              SPEED          MSS                RX      TX
VPN  INTERFACE  TYPE  IP ADDRESS        STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR
              MBPS   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------------
0    ge0/0      ipv4  10.66.15.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:62  1000   full    1420    0:14:05:30  546018   545562
0    ge0/1      ipv4  10.1.17.15/24     Up      Up      null   service    1500
00:0c:29:db:f0:6c  1000   full    1420    0:14:21:42  0        10
0    ge0/2      ipv4  -                 Down    Up      null   service    1500
00:0c:29:db:f0:76  1000   full    1420    0:14:22:10  0        0
0    ge0/3      ipv4  10.0.20.15/24     Up      Up      null   service    2000
00:0c:29:db:f0:80  1000   full    1920    0:14:21:42  0        10
0    ge0/6      ipv4  172.17.1.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:9e  1000   full    1420    0:14:21:42  0        10
0    ge0/7      ipv4  10.0.100.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:a8  1000   full    1420    0:14:21:42  773      708
0    system     ipv4  172.16.255.15/32  Up      Up      null   loopback   1500
00:00:00:00:00:00  0      full    1420    0:14:21:54  0        0
0    loopback3  ipv4  10.1.15.15/24     Up      Up      null   transport  2000
00:00:00:00:00:00  10     full    1920    0:14:21:46  0        0
```

```
1    ge0/4      ipv4  10.20.24.15/24    Up      Up      null   service    2000
00:0c:29:db:f0:8a  1000   full    1920    0:14:21:38  52038    52079
1    ge0/5      ipv4  172.16.1.15/24    Up      Up      null   service    1500
00:0c:29:db:f0:94  1000   full    1420    0:14:21:38  0        8
512  eth0       ipv4  10.0.1.15/24      Up      Up      null   service    1500
00:50:56:00:01:05  0      full    0       0:14:21:39  28926    29663
```

The following instances support jumbo frames:

- Accelerated computing—CG1, G2, P2
- Compute optimized—C3, C4, CC2
- General purpose—M3, M4, T2
- Memory optimized—CR1, R3, R4, X1
- Storage optimized—D2, HI1, HS1, I2

What's Next

See *Install Signed Certificates on vEdge Cloud Routers*.

Create vEdge Cloud router VM Instance on Azure

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on Microsoft Azure. You can also create the VM on Amazon AWS or on a server running the vSphere ESXi Hypervisor software or the Kernel-based Virtual Machine (KVM) Hypervisor software.

Note: Cisco Catalyst SD-WAN offers only a Bring Your Own License (BYOL) for the vEdge Cloud router, so you are not actually purchasing the Cisco Catalyst SD-WAN product. You are charged hourly for the VNET instance.

For server requirements, see Server Hardware Recommendations.

Launch Azure Marketplace and Create a vEdge Cloud router VM Instance

1. Launch the Azure Marketplace application:
   a. In the left pane, click **New** to create a new vEdge Cloud router VM instance.
   b. In the **Search** box, search for **Cisco**.
2. In the right pane, select Cisco vEdge Cloud router (3 NICs) (Staged).
3. In the Cisco vEdge Cloud router (3 NICs) (Staged) screen, click **Basics** in the left pane to configure basic settings for the vEdge Cloud router VM:
   a. In the **VM Name** field, enter a name for the vEdge Cloud router VM instance.
   b. In the **Username** field, enter the name of a user who can access the VM instance.
   c. In the **Authentication type** field, select either **Password** or **SSH public key**.
   d. If you selected password, enter, and then confirm, your password. You use the username and password to open SSH session to the VM instance.

e. If you selected SSH public key, see https://docs.microsoft.com/en-us/azu...reate-ssh-keys for instructions about how to generate an SSH key pair for Linux VMs.

f. In the **Subscription** field, select **Pay-As-You-Go** from the drop-down menu.

g. In the **Resource Group** field, click **Create new** to create a new resource group, or click **Use existing** to select an existing resource group from the drop-down menu.

h. In the **Location** field, select the location in which you wish to bring up the vEdge Cloud router VM instance.

i. Click **OK**.

4. In the left pane, click **vEdge Settings** to configure the vEdge Cloud router infrastructure settings.

5. In the Infrastructure Settings pane:

a. Click **Size**. In the **Choose a size** pane, select D3_V2 Standard for the instance type and click **Select**. This is the recommended instance type.

b. Click **Storage Account**. In the **Choose storage account** pane, click **Create New** to create a new storage account or select one of the listed storage accounts. Then click **OK**.

c. Click **Public IP Address**. In the **Choose public IP address** pane, click **Create New** to create a new public IP address, or select one of the listed public IP address to use for the public IP subnet. Then click **OK**.

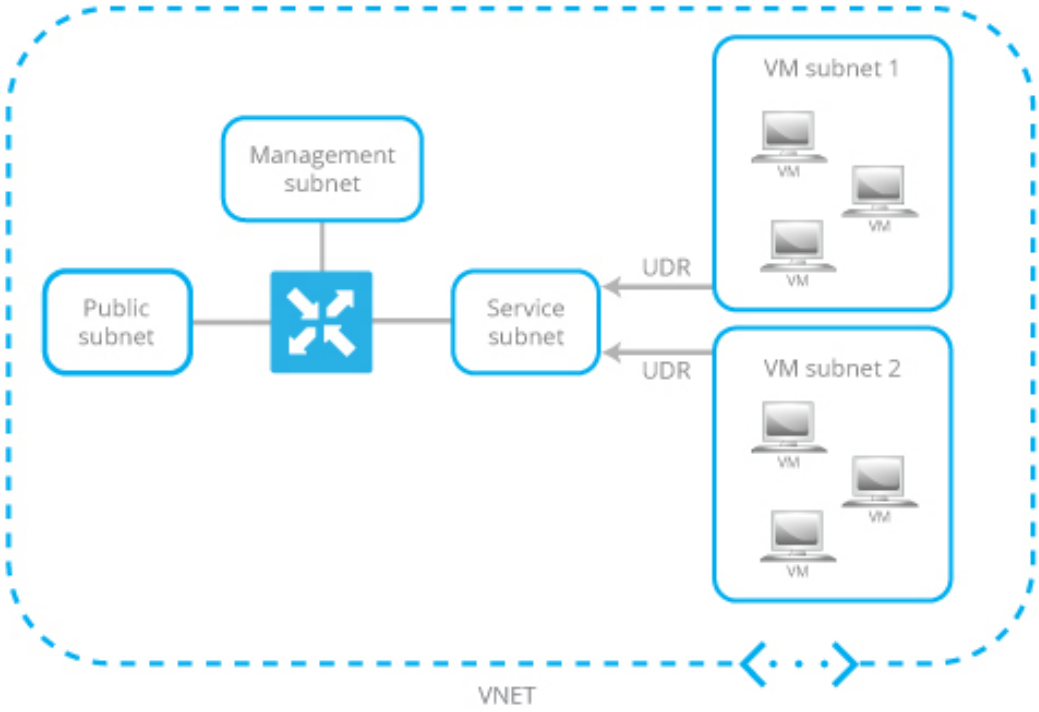
d. In the **Domain Name** field, select **vedge** from the drop-down menu.

e. Click **Virtual Network**. In the **Choose virtual network** pane, click **Create New** to create a new virtual network (VNET), or select an existing VNET to launch the vEdge Cloud instance in. Then click **OK**.

f. If you selected an existing VNET, use the drop-down menu to choose available subnets within the VNET. Then click **OK**.

You must have three subnets available within the VNET; otherwise, the vEdge Cloud router VM instance will fail to launch. Also, ensure that route tables associated with your VM subnets have a user-defined route (UDR) towards the service subnet of the vEdge Cloud router. The UDR ensures that the VM subnets use the vEdge Cloud router as the gateway. See the example topology below.

Figure 26: Example Topology of VNET with VM Subnets



g. If you created a new VNET, define the address space within that VNET. Then click **OK** in the Subnets pane.

Cisco Catalyst SD-WAN prepopulates subnet names and assigns IP addresses per subnet from the VNET address space you defined. If you plan to connect your VNET instances through the service subnet associated to the vEdge Cloud router, you do not need to make updates to the route table.

6. In the Summary pane, click **OK**. The Summary pane validates and displays the configuration you defined for the vEdge Cloud router VM instance.

7. Click **Buy to purchase**. Then click **Purchase** in the **Purchase** pane.

Note Cisco Catalyst SD-WAN offers only a Bring Your Own License (BYOL) for the vEdge Cloud router, so you are not actually purchasing the Viptela product. You are charged hourly for the VNET instance.

The system creates the vEdge Cloud router VM instance and notifies you that the deployment has succeeded.

8. Click the **vEdge VM** instance you just created.

The system displays the public IP address and DNS name of the vEdge Cloud router VM instance.

9. SSH into the public IP address of the vEdge Cloud router VM instance.

10. At the login prompt, log in with the username and password you created in Step 3. To view the vEdge Cloud router default configuration, enter the following command:

```
vEdge# show running-config
```

When you create a vEdge Cloud router VM, the security group configuration shown below is applied to the NIC associated with the public subnet. This security group does not restrict traffic from specific sources, but it does restrict specific services. Custom services for TCP and UDP that need to be enabled for Cisco Catalyst SD-WAN control protocols are also automatically configured. You can change the security group configuration to suit your requirements.

vEdge Cloud Router Interface and Subnet Mapping

To create a vEdge Cloud router VM instance on Azure Marketplace, a minimum of three NICs are required—one each for management, service, and transport. The table below shows the mapping of the vEdge Cloud router interface with the subnet associated to these NICs.

vEdge Cloud Router Interface	Subnet	Description
eth0	Management subnet	In-band management
ge0/1	Service subnet	Connects the vEdge Cloud router as a gateway device
ge0/0	Transport subnet	Transport/WAN link

What's Next

See *Install Signed Certificates on vEdge Cloud Routers*.

Create vEdge Cloud VM Instance on ESXi

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on a server running the vSphere ESXi Hypervisor software. You can also create the VM on Amazon AWS or on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software.

For server requirements, see Server Hardware Recommendations.

To create a vEdge Cloud VM instance on the ESXi hypervisor:

1. Launch the vSphere Client and create a vEdge Cloud VM instance.
2. Add a vNIC for the tunnel interface.
3. Start the vEdge Cloud VM instance and connect to the console.

The details of each step are provided below.

If you are using the VMware vCenter Server to create the vEdge Cloud VM instance, follow the same procedure. Note, however, that the vCenter Server screens look different than the vSphere Client screens shown in the procedure.

Launch vSphere Client and Create a vEdge Cloud VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the EXSi server, your username, and your password. Click Login to log in to the ESXi server.

The system displays the ESXi screen.

2. Click **File** > **Deploy OVF Template** to deploy the virtual machine.
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vedge.ova file that you downloaded from Cisco. Then click **Next**.
4. Click **Next** to verify OVF template details.
5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the vEdge instance.
6. Click **Next** to accept the default format for the virtual disks.
7. Click **Next** to accept your destination network name as the destination network for the deployed OVF template. In the figure below, CorpNet is the destination network.
8. In the Ready to Complete screen, click **Finish**.

   The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes four vNICs which can be used for the management, tunnel, or service interface.

Add a New vNIC

1. In the left navigation bar of the vSphere Client, select the vEdge Cloud VM instance you just created, and click **Edit virtual machine settings**.
2. In the vEdge Cloud – Virtual Machine Properties screen, click **Add** to add a new vNIC. Then click **OK**.
3. Click Ethernet Adapter for the type of device you wish to add. Then click **Next**.
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.
5. In the Ready to Complete screen, click **Finish**.
6. The vEdge Cloud – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.

Modify the MTU for a vSwitch

To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU for each virtual switch (vSwitch):

1. Launch the ESXi Hypervisor and select the **Configuration** tab.
2. In the **Hardware** field, click **Networking**. The network adapters you added are displayed in the right pane.
   a. Click **Properties** for the vSwitch whose MTU you wish to modify.
3. In the vSwitch Properties screen, click **Edit**.
4. In the **Advanced Properties MTU** drop-down, change the vSwitch MTU to the desired value. The range is 2000 to 9000. Then click **OK**.

Start the vEdge Cloud VM Instance and Connect to the Console

1. In the left navigation bar of the vSphere Client, select the vEdge Cloud VM instance you just created, and click **Power** on the virtual machine. The vEdge Cloud virtual machine is powered on.
2. Select the **Console** tab to connect to the vEdge Cloud console.
3. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**. To view the vEdge Cloud router default configuration, enter the following command:

```
vEdge# show running-config
```

Mapping vNICs to Interfaces

When you create a vEdge Cloud router VM instance on ESXi in the procedure in the previous section, you create two vNICs: vNIC 1, which is used for the management interface, and vNIC 2, which is used as a tunnel interface. From the perspective of the VM itself, these two vNICs map to the eth0 and eth1 interfaces, respectively. From the perspective of the Cisco Catalyst SD-WAN software for the vEdge Cloud router, these two vNICs map to the mgmt0 interface in VPN 512 and the ge0/0 interface in VPN 0, respectively. You cannot change these mappings.

You can configure up to five additional vNICs, numbered 3 through 7, on the VM host. You can map these vNICs to interfaces eth2 through eth7 as desired, and to Cisco Catalyst SD-WAN interfaces ge0/1 through ge0/7, as desired.

The table below summarizes the mapping between vNICs, VM host interfaces, and vEdge Cloud interfaces.

Table 28:

vNIC	Interface on VM Host	Interface in vEdge Cloud Configuration
vNIC 1	eth0	mgmt0 in VPN 512
vNIC 2	eth1	ge0/0
vNIC 3 through 7	eth2 through eth7	ge0/1 through ge0/7

Note The traffic destined to VRRP IP is not forwarded by ESXi, since VRRP MAC address is not learned by the Virtual Software Switch of ESXi associated with the vEdge Ethernet interface. This is due to the limitation of the VMWare ESXi, which does not allow multiple unicast MAC address configuration on vNIC. As a workaround, place the vNIC in promiscuous mode and perform MAC filtering in the software. To let Cisco vEdge software place interface in promiscuous mode, Virtual Software Switch port-group or switch configuration must be changed to allow the same. Be aware that ESXi VSS forwards all packets to all virtual machines that are connected to the port-group or switch. This can have an adverse performance impact on the ESXi Host other virtual machines. This might also have an adverse effect on the vEdge packet processing performance. Design your network carefully to avoid performance impact.

What's Next

See *Install Signed Certificates on vEdge Cloud Routers*.

Create vEdge Cloud VM Instance on KVM

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software. You can also create the VM on Amazon AWS or on a server running the vSphere ESXi Hypervisor software.

For server requirements, see *Server Hardware Recommendations*.

Create vEdge Cloud VM Instance on the KVM Hypervisor

To create a vEdge Cloud VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager screen.
2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine screen.
3. Enter the name of the virtual machine. The figure below specifies a name for the vEdge Cloud instance.
   a. Select **Import existing disk image**.
   b. Click **Forward**.
4. In **Provide the existing storage path** field, click **Browse to find the vEdge Cloud software image**.
   a. In the **OS Type** field, select **Linux**.
   b. In the **Version** field, select the Linux version you are running.
   c. Click **Forward**.
5. Specify Memory and CPU based on your network topology and the number of sites. Click **Forward**.
6. Select **Customize configuration before install**. Then click **Finish**.
7. Select **Disk 1** in the left navigation bar. Then:
   a. Click **Advanced Options**.
   b. In the **Disk Bus** field, select **IDE**.
   c. In the **Storage Format** field, select **qcow2**.
   d. Click **Apply** to create the VM instance with the parameters you just defined. By default, this includes one vNIC. This vNIC is used for the management interface.



Note Cisco Catalyst SD-WAN software supports VMXNET3 and Virtio vNICs. It is recommended, however, that you use the Virtio vNICs.

8. In the vEdge Cloud Virtual Machine screen, click **Add Hardware** to add a second vNIC for the tunnel interface.
9. In the Add New Virtual Hardware screen, click **Network**.

a. In the **Host Device** field, select an appropriate host device.

b. Click **Finish**.

The newly created vNIC is listed in the left pane. This vNIC is used for the tunnel interface.

10. Create an ISO file to include a cloud-init configuration for the vEdge Cloud router.



Note Starting from Cisco SD-WAN Release 20.7.1, the cloud-init configuration file should only contain the minimum configuration required for setting up control connections to Cisco SD-WAN Manager. Other configuration such as the VPN0 and clear-text passwords should be pushed through the Add-On CLI template on Cisco SD-WAN Manager.

11. In the Virtual Machine Manager screen, click Add Hardware to attach the ISO file you created.

12. In the Add New Virtual Hardware screen:

a. Click **Select** managed or other existing storage.

b. Click **Browse** and select the ISO file you created.

c. In the **Device type** field, select IDE CDROM.

d. Click **Finish**.

13. To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU for each virtual network (vnet) and virtual bridge NIC-containing VNET (virbr-nic) interface to a value in the range of 2000 to 9000:

a. From the VM shell, issue the following command to determine the MTU on the vnet and virbr-nic interfaces:

```
user@vm:~$ ifconfig -a
virbr1-nic Link encap:Ethernet HWaddr 52:54:00:14:4e:6f
          BROADCAST MULTICAST  MTU:1500  Metric
          RX packets:0 errors:0 dropped:0 ovreruns:0 frame:0
          TX packets:0 errors:0 dropped:0 ovreruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0B)
...
vnet0     Link encap:Ethernet  HWaddr fe:50:56:00:10:1e
          inet6 addr: fe80::fc50:56ff:fe00:11e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:167850 errors:0 dropped:0 overruns:0 frame:0
          TX packets:663186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19257426 (19.2 MB)  TX bytes:42008544 (42.0 MB)
...
```

b. Change the MTU of each vnet:

```
user@vm:~$ sudo ifconfig vnet number mtu 2000
```

c. Change the MTU of each virbr-nic:

```
user@vm:~$ sudo ifconfig virbr-nic number mtu 2000
```

d. Verify the MTU value:

```
user@vm:~$ ifconfig -a
```

14. In the vEdge Cloud Virtual Machine page, click **Begin Installation** in the top upper-left corner of the screen.
15. The system creates the virtual machine instance and displays the vEdge Cloud console.
16. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**. To view the vEdge Cloud router default configuration, enter the following command:

    ```
    vEdge# show running-config
    ```

Note that the Cisco Catalyst SD-WAN software supports VMXNET3 and Virtio vNICs. It is recommended, however, that you use the Virtio vNICs.

Mapping vNICs to Interfaces

When you create a vEdge Cloud router VM instance on KVM in the procedure in the previous section, you create two vNICs: vNIC 1, which is used for the management interface, and vNIC 2, which is used as a tunnel interface. From the perspective of the VM itself, these two vNICs map to the eth0 and eth1 interfaces, respectively. From the perspective of the Cisco Catalyst SD-WAN software for the vEdge Cloud router, these two vNICs map to the mgmt0 interface in VPN 512 and the ge0/0 interface in VPN 0, respectively. You cannot change these mappings.

You can configure up to five additional vNICs, numbered 3 through 7, on the VM host. You can map these vNICs to interfaces eth2 through eth7 as desired, and to Cisco Catalyst SD-WAN interfaces ge0/1 through ge0/7, as desired.

The table below summarizes the mapping between vNICs, VM host interfaces, and vEdge Cloud interfaces.

Table 29:

vNIC	Interface on VM Host	Interface in vEdge Cloud Configuration
vNIC 1	eth0	mgmt0 in VPN 512
vNIC 2	eth1	ge0/0
vNIC 3 through 7	eth2 through eth7	ge0/1 through ge0/7

What's Next

See *Install Signed Certificates on Edge Cloud Routers*.

Configure Certificate Authorization Settings for WAN Edge Routers

Certificates are used to authenticate routers in the overlay network. Once authentication is complete, the routers can establish secure sessions with other devices in the overlay network.

By default, the WAN Edge Cloud Certificate Authorization is automated. This is the recommended setting.

If you use third-party certificate authorization, configure certificate authorization to be manual:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.

2. Click **Hardware WAN Edge Certificate Authorization**. (If you are usingCisco Catalyst SD-WAN Manager Release 20.12.1 or ealier, click **Edit**.
3. In the **Security**, select Enterprise Certificate (signed by Enterprise CA).
4. Click **Save**.

Install Signed Certificates on vEdge Cloud Routers

When a vEdge Cloud router virtual machine (VM) instance starts, it has a factory-default configuration, which allows the router to boot. However, the router is unable to join the overlay network. For the router to be able to join the overlay network, you must install a signed certificate on the router. The signed certificates are generated based on the router's serial number, and they are used to authorize the router to participate in the overlay network.

Starting from Releases 17.1, the Cisco SD-WAN Manager can act as a Certificate Authority (CA), and in this role it can automatically generate and install signed certificates on vEdge Cloud routers. You can also use another CA and then install the signed certificate manually. For Releases 16.3 and earlier, you manually install signed Symantec certificates on vEdge Cloud routers.

To install signed certificates:

1. Retrieve the vEdge authorized serial number file. This file contains the serial numbers of all the vEdge routers that are allowed to join the overlay network.
2. Upload the vEdge authorized serial number file to Cisco SD-WAN Manager.
3. Install a signed certificate on each vEdge Cloud router.

Retrieve vEdge Authorized Serial Number File

1. Go to http://viptela.com/support/ and log in.
2. Click **Downloads**.
3. Click **My Serial Number Files**. The screen displays the serial number files. Starting from Releases 17.1, the filename extension is .viptela. For Releases 16.3 and earlier, the filename extension is .txt.
4. Click the most recent serial number file to download it.

Upload vEdge Authorized Serial Number File

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. Click **vEdge List**, and select **Upload vEdge List**.
3. In the Upload vEdge window:
   a. Click **Choose File**, and select the vEdge authorized serial number file you downloaded from Cisco.
   b. To automatically validate the vEdge routers and send their serial numbers to the controllers, click and select the checkbox **Validate the Uploaded vEdge List** and **Send to Controllers**. If you do not select this option, you must individually validate each router in the **Configuration** > **Certificates** > **vEdge List** page.

4. Click **Upload**.

During the process of uploading the vEdge authorized serial number file, the Cisco SD-WAN Manager generates a token for each vEdge Cloud router listed in the file. This token is used as a one-time password for the router. The Cisco SD-WAN Manager sends the token to the Cisco SD-WAN Validator and the Cisco SD-WAN Controller.

After the vEdge authorized serial number file has been uploaded, a list of vEdge routers in the network is displayed in the vEdge Routers Table in the **Configuration** > **Devices** page, with details about each router, including the router's chassis number and its token.

Install Signed Certificates in Releases 17.1 and Later

Starting from Releases 17.1, to install a signed certificates on a vEdge Cloud router, you first generate and download a bootstrap configuration file for the router. This file contains all the information necessary to allow the Cisco SD-WAN Manager to generate a signed certificate for the vEdge Cloud router. You then copy the contents of this file into the configuration for the router's VM instance. For this method to work, the router and the Cisco SD-WAN Manager must both be running Release 17.1 or later. Finally, you download the signed certificate to the router. You can configure the Cisco SD-WAN Manager to do this automatically or manually.

The bootstrap configuration file contains the following information:

- UUID, which is used as the router's chassis number.
- Token, which is a randomly generated one-time password that the router uses to authenticate itself with the Cisco SD-WAN Validator and the Cisco SD-WAN Manager.
- IP address or DNS name of the Cisco SD-WAN Validator.
- Organization name.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1 you cannot include a comma in the **Organization Name** field of the bootstrap configuration file.
- If you have already created a device configuration template and attached it to the vEdge Cloud router, the bootstrap configuration file contains this configuration. For information about creating and attaching a configuration template, see Create Configuration Templates for a vEdge Router .

You can generate a bootstrap configuration file that contains information for an individual router or for multiple routers.

Starting from Releases 17.1, you can also have Symantec generate signed certificates that you install manually on each router, as described later in this article, but this method is not recommended.

Configure the Cisco Catalyst SD-WAN Validator and Organization Name

Before you can generate a bootstrap configuration file, you must configure the Cisco SD-WAN Validator DNS name or address and your organization name:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. Click **Validator**. (click **Edit**.)
3. In the **DNS/IP Address: Port field**, enter the DNS name or IP address of the Cisco SD-WAN Validator.
4. Click **Save**.

5. Verify the orgnization name. This name must be identical to that configured on the Cisco SD-WAN Validator. (If your are using Cisco Catalyst SD-WAN Manager Release 20.12.1 or earlier, to verify **Organization Name**, click **View**.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, the system Organization Name cannot contain a comma. Comma is not allowed during the device configuration.

6. Click **Save**.

Configure Automatic or Manual vEdge Cloud Authorization

Signed certificates must be installed on each vEdge cloud router so that the router is authorized to participate in the overlay network. You can use the Cisco SD-WAN Manager as the CA to generate and install the signed certificate, or you can use an enterprise CA to install the signed certificate.

It is recommended that you use the Cisco SD-WAN Manager as a CA. In this role, Cisco SD-WAN Manager automatically generates and installs a signed certificate on the vEdge Cloud router. Having Cisco SD-WAN Manager act as a CA is the default setting. You can view this setting in the WAN vEdge Cloud Certificate Authorization, on the Cisco SD-WAN Manager **Administration** > **Settings** page.

To use an enterprise CA for generating signed certificates for vEdge Cloud routers:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. Click **WAN Edge Cloud Certificate Authorization** and select **Manual**.
3. Click **Save**.

Generate a Bootstrap Configuration File

Note In Cisco SD-WAN Release 20.5.1, the cloud-init bootstrap configuration that you generate for the Cisco vEdge Cloud router cannot be used for deploying Cisco vEdge Cloud router 20.5.1. However, you can use the bootstrap configuration for deploying Cisco vEdge Cloud router 20.4.1 and the earlier versions.

To generate a bootstrap configuration file for a vEdge Cloud router:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. To generate a bootstrap configuration file for one or multiple vEdge Cloud routers:
   a. Click **WAN Edge List**, select **Export Bootstrap Configuration**.
   b. In the Generate Bootstrap Configuration field, select the file format:
      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select **Cloud-Init** to generate a token, Cisco SD-WAN Validator IP address, vEdge Cloud router UUID, and organization name.

        Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, the system Organization Name cannot contain a comma. Comma is not allowed during the device configuration.

      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.

c. From the **Available Devices** column, select one or more routers.

d. Click the arrow pointing to right to move the selected routers to **Selected Devices** column.

e. Click **Generate Generic Configuration**. The bootstrap configuration is downloaded in a .zip file, which contains one .cfg file for each router.

3. To generate a bootstrap configuration file individually for each vEdge Cloud router:

a. Click **WAN Edge List**, select the desired vEdge Cloud router.

b. For the desired vEdge Cloud router, click **...**, and select **Generate Bootstrap Configuration**.

c. In the **Generate Bootstrap Configuration** window, select the file format:

- For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select Cloud-Init to generate a token, Cisco SD-WAN Validator IP address, vEdge Cloud router UUID, and organization name.
- For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.

Note Beginning with Cisco vManage Release 20.7.1, there is an option available when generating a bootstrap configuration file for a Cisco vEdge device, enabling you generate two different forms of the bootstrap configuration file.

- If you are generating a bootstrap configuration file for a Cisco vEdge device that is using Cisco Catalyst SD-WAN Release 20.4.x or earlier, then check the **The version of this device is 20.4.x or earlier** check box.
- If you are generating a bootstrap configuration for a Cisco vEdge device that is using Cisco SD-WAN Release 20.5.1 or later, then do not use the check box.

d. Click **Download** to download the bootstrap configuration. The bootstrap configuration is downloaded in a .cfg file.

Then use the contents of the bootstrap configuration file to configure the vEdge Cloud router instance in AWS, ESXi, or KVM. For example, to configure a router instance in AWS, paste the text of the Cloud-Init configuration into the User data field:

By default, the **ge0/0** interface is the router's tunnel interface, and it is configured as a DHCP client. To use a different interface or to use a static IP address, and if you did not attach a device configuration template to the router, change the vEdge Cloud router's configuration from the CLI. See *Configuring Network Interfaces*.

Install the Certificate on the vEdge Cloud Router

If you are using automated vEdge Cloud certificate authorization, which is the default, after you configure the vEdge Cloud router instance, Cisco SD-WAN Manager automatically installs a certificate on the router and the router's token changes to its serial number. You can view the router's serial number in the **Configuration** > **Devices** page. After the router's control connections to the Cisco SD-WAN Manager come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

   ```
   vEdge# request root-cert-chain install filename [vpn vpn-id]
   ```

   Then, Cisco SD-WAN Manager generates a CSR.

2. Download the CSR:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. For the selected vEdge Cloud router for which to sign a certificate, click **...** and select **View CSR**.
   c. To download the CSR, click **Download**.
3. Send the certificate to a third-party signing authority, to have them sign it.
4. Import the certificate into the device:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. Click **Controllers**, and select **Install Certificate**.
   c. In the **Install Certificate** page, paste the certificate into the Certificate Text field, or click **Select a File** to upload the certificate in a file.
   d. Click **Install**.
5. Issue the following REST API call, specifying the IP address of your Cisco SD-WAN Manager:

   ```
   https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain
   ```

Create the vEdge Cloud Router Bootstrap Configuration from the CLI

It is recommended that you generate the vEdge Cloud router's bootstrap configuration using Cisco SD-WAN Manager. If, for some reason, you do not want to do this, you can create the bootstrap configuration using the CLI. With this process, you must still, however, use Cisco SD-WAN Manager. You collect some of this information for the bootstrap configuration from Cisco SD-WAN Manager, and after you have created the bootstrap configuration, you use Cisco SD-WAN Manager to install the signed certificate on the router.

Installing signed certificates by creating a bootstrap configuration from the CLI is a three-step process:

1. Edit the router's configuration file to add the DNS name or IP address of the Cisco SD-WAN Validator and your organization name.
2. Send the router's chassis and token numbers to Cisco SD-WAN Manager.
3. Have Cisco SD-WAN Manager authenticate the vEdge Cloud router and install the signed certificate on the router.

To edit the vEdge Cloud router's configuration file from the CLI:

1. Open a CLI session to the vEdge Cloud router via SSH. To do this in Cisco SD-WAN Manager, select **Tools** > **SSH Terminal** page, and select the desired router.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

```
vEdge# config
vEdge(config)#
```

4. Configure the IP address of the Cisco SD-WAN Validator or a DNS name that points to the Cisco SD-WAN Validator. The Cisco SD-WAN Validator's IP address must be a public IP address:

   ```
   vEdge(config)# system vbond (dns-name | ip-address)
   ```

5. Configure the organization name:

   ```
   vEdge(config-system)# organization-name name
   ```

6. Commit the configuration:

   ```
   vEdge(config)# commit and-quit
   vEdge#
   ```

To send the vEdge Cloud router's chassis and token numbers to Cisco SD-WAN Manager:

1. Locate the vEdge Cloud router's token and chassis number:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
   b. Click **WAN Edge List**, locate the vEdge Cloud router.
   c. Make a note of the values in the vEdge Cloud router's Serial No./Token and Chassis Number columns.
2. Send the router's bootstrap configuration information to Cisco SD-WAN Manager:

   ```
   vEdge# request vedge-cloud activate chassis-number chassis-number token token-number
   ```

Issue the **show control local-properties** command on the router to verify the Cisco SD-WAN Validator IP address, the organization name the chassis number, and the token. You can also verify whether the certificate is valid.

Finally, have Cisco SD-WAN Manager authenticate the vEdge Cloud router and install the signed certificate on the router.

If you are using automated vEdge Cloud certificate authorization, which is the default, the Cisco SD-WAN Manager uses the chassis and token numbers to authenticate the router. Then, Cisco SD-WAN Manager automatically installs a certificate on the router and the router's token changes to a serial number. You can display the router's serial number in the **Configuration** > **Devices** page. After the router's control connections to Cisco SD-WAN Manager come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

   ```
   vEdge# request root-cert-chain install filename [vpn vpn-id]
   ```

   After you install the root chain certificate on the router, and after Cisco SD-WAN Manager receives the chassis and token numbers, Cisco SD-WAN Manager generates a CSR.

2. Download the CSR:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. For the selected vEdge Cloud router for which to sign a certificate, click **...** and select **View CSR**.
   c. To download the CSR, click **Download**.

3. Send the certificate to a third-party signing authority, to have them sign it.
4. Import the certificate into the device:
   a. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
   b. Click Controllers and select **Install Certificate**.
   c. In the **Install Certificate** page, paste the certificate into the Certificate Text field, or click **Select a File** to upload the certificate in a file.
   d. Click **Install**.
5. Issue the following REST API call, specifying the IP address of your Cisco SD-WAN Manager:

   https://*vmanage-ip-address*/**dataservice/system/device/sync/rootcertchain**

Install Signed Certificates in Releases 16.3 and Earlier

For vEdge Cloud router virtual machine (VM) instances running Releases 16.3 and earlier, when the vEdge Cloud router VM starts, it has a factory-default configuration, but is unable to join the overlay network because no signed certificate is installed. You must install a signed Symantec certificate on the vEdge Cloud router so that it can participate in the overlay network.

To generate a certificate signing request (CSR) and install the signed certificate on the vEdge Cloud router:

1. Log in to the vEdge Cloud router as the user **admin**, using the default password, **admin**. If the vEdge Cloud router is provided through AWS, use your AWS key pair to log in. The CLI prompt is displayed.
2. Generate a CSR for the vEdge Cloud router:

   ```
   vEdge# request csr upload path
   ```

   path is the full path and filename where you want to upload the CSR. The path can be in a directory on the local device or on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided. When prompted, enter and then confirm your organization name. For example:

   ```
   vEdge# request csr upload home/admin/vm9.csr
   Uploading CSR via VPN 0
   Enter organization name            : Cisco
   Re-enter organization name         : Cisco
   Generating CSR for this vEdge device
   ........[DONE]
   Copying ... /home/admin/vm9.csr via VPN 0
   CSR upload successful
   ```

3. Log in to the Symantec Certificate Enrollment portal:

   https://certmanager.<wbr>websecurity.symantec.com/<wbr>mcelp/enroll/index?jur_hash=<wbr>f422d7ceb508a24e32ea7de4f78d37<wbr>f8

4. In the **Select Certificate Type** drop-down, select **Standard Intranet SSL** and click **Go**. The Certificate Enrollment page is displayed. Cisco Catalyst SD-WAN uses the information you provide on this form to confirm the identity of the certificate requestor and to approve your certificate request. To complete the Certificate Enrollment form:
   a. In the Your Contact Information section, specify the First Name, Last Name, and Email Address of the requestor.

b. In the Server Platform and Certificate Signing section, select Apache from the Select Server Platform drop-down. In the Enter Certificate Signing Request (CSR) box, upload the generated CSR file, or copy and paste the contents of the CSR file. (For details about how to do this, log in to support.viptela.com. Click Certificate, and read the Symantec certificate instructions.)

c. In the Certificate Options section, enter the validity period for the certificate.

d. In the Challenge Phrase section, enter and then re-enter a challenge phrase. You use the challenge phrase to renew, and, if necessary, to revoke a certificate on the Symantec Customer Portal. It is recommended that you specify a different challenge phrase for each CSR.

e. Accept the Subscriber Agreement. The system generates a confirmation message and sends an email to the requestor confirming the certificate request. It also sends an email to the Cisco to approve the CSR.

5. After Cisco approves the CSR, Symantec sends the signed certificate to the requestor. The signed certificate is also available through the Symantec Enrollment portal.

6. Install the certificate on the vEdge Cloud router:

```
vEdge# request certificate install filename [vpn vpn-id]
```

The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided.

7. Verify that the certificate is installed and valid:

```
vEdge# show certificate validity
```

After you have installed the certificate on the vEdge Cloud router, the Cisco SD-WAN Validator is able to validate and authenticate the router, and the router is able to join the overlay network.

What's Next

See *Send vEdge Serial Numbers to the Controller Devices*.

Send Router Serial Numbers to the Controller Devices

Table 30: Feature History

Feature Name	Release Information	Description
Device Onboarding Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature provides an enhancement to onboard your device to Cisco SD-WAN Manager by directly uploading a .csv file.

Only authorized routers can join the overlay network. The controller devices Cisco SD-WAN Manager, Cisco SD-WAN Controllers and Cisco SD-WAN Validators learn which routers are authorized to join the overlay network from the router-authorized serial number file. This is a file that you receive from Cisco. The router authorized serial number file lists the serial numbers and corresponding chassis numbers for all authorized routers. Upload the file to one of the Cisco SD-WAN Manager in your network, and it then distributes the file to the controllers.

When you upload the router serial number file, you can place the routers in one of these states:

- Invalid: When you power on the routers, they are not authorized to join the overlay network.
- Staging: When you power on the routers, they are validated and authorized to join the overlay network, and can establish connections only to the control plane. Over the control plane, the routers receive their configuration from Cisco SD-WAN Manager. However, the routers are unable to establish data plane connections, so they cannot communicate with other routers in the network. The Staging state is useful when you are preparing routers at one location and then sending them to different sites for installation. Once the routers reach their final destination, you change their state from Staging to Valid, to allow the routers to establish data plane connections and to fully join the overlay network.
- Valid: When you power on the routers, they are validated and authorized to join the overlay network, and they are able to establish both control plane and data plane connections in the network. Over the control plane, the routers receive their configuration from Cisco SD-WAN Manager. Over the data plane, they are able to communicate with other routers. The Valid state is useful when the routers are being installed at their final destination.



Note To successfully send a router serial number file to Cisco Catalyst SD-WAN Manager in Cisco vManage Release 20.10.1 and earlier, ensure that the file is installed in `/home/admin` or `/home/vmanage-admin`. Using credentials other than **admin** or **vmanage-admin** to send a router serial number file will result in an error.

How to Upload a Router Authorized Serial Number File

The following sections describe how to upload the router authorized serial number file to Cisco SD-WAN Manager and distribute the file to all the overlay network controllers.

Enable PnP Connect Sync (Optional)

To sync the uploaded device to your Smart Account or Virtual Account and for your device to reflect on the PnP (Plug and Play) Connect portal, when an unsigned .csv file is uploaded through Cisco SD-WAN Manager, enable the PnP Connect Sync.

Ensure you have an active connection to the PnP (Plug and Play) Connect portal and an active Smart Account and Virtual Account. You have to also use a CCO ID that is associated as the Smart Account or Virtual Account admin of the account, on PnP Connect portal.



Note PnP Connect Sync is only applicable to .csv file upload. It does not affect the .viptela file (which is downloaded from the PnP Connect portal) upload process.



Note You will be allowed to enable PnP Connect Sync only once you enter the Smart Account credentials.

To enable the PnP Connect Sync:

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.

2. Click **Smart Account Credentials**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier, click **Edit.**.)
3. Enter **Username** and **Password** and click **Save.**
4. Click **PnP Connect Sync**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier, click **Edit.**.)
5. Click **Enabled** and click **Save.**

Place Routers in Valid State

Perform the following task to place the routers in the Valid state so that they can establish control and data plane connections and can receive their configurations from the Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. Click **WAN Edge List** and click **Upload WAN Edge List**.
3. You can upload WAN Edge devices in the following two ways:
   - Upload a signed file (.viptela file). You can download this .viptela file from the Plug and Play Connect portal.
   - Starting from Cisco vManage Release 20.3.1, you can upload an unsigned file (.csv file). This enhancement is only applicable when you add hardware platforms on-demand onto Cisco SD-WAN Manager. To upload the .csv file this:
     a. Click **Sample CSV**. An excel file will be downloaded.
     b. Open the downloaded .csv file. Enter the following parameters:
        - Chassis number
        - Product ID (mandatory for Cisco vEdge devices, blank value for all other devices)
        - Serial number
        - SUDI serial

        Either the Serial number or SUDI number is mandatory for Cisco IOS XE Catalyst SD-WAN devices, along with chassis number. Cisco ASR1002-X is an exception and does not need Serial or SUDI numbers, it can be onboarded with only the chassis number on the .csv file.
     c. To view your device details in Cisco SD-WAN Manager, go to **Tools** > **SSH Terminal**. Choose your device and use one of the following command-

        show certificate serial (for vEdge devices)

        show sdwan certificate serial (for Cisco IOS XE Catalyst SD-WAN devices)
     d. Enter the specific device details in the downloaded .csv file.
4. To upload the .viptela or .csv file on Cisco SD-WAN Manager click **Choose file** and upload the file that contains the product ID, serial number and chassis number of your device.

Note If you have enabled PnP Sync Connect, the .csv file can contain upto 25 devices. If you have more than 25 devices, you can split them and upload multiple files.

5. Check the check box next to **Validate the uploaded vEdge List and send to controllers**.
6. Click **Upload.**
7. You should now see your device listed in the table of devices.

   If you have enabled the PnP Sync Connect previously, your device will also reflect on the PnP Portal.

A list of routers in the network is displayed, showing detailed information about each router. To verify that the routers are in the Valid state, select **Configuration** > **Certificates.**

Place Routers in Invalid State

To upload the authorized serial number file to the Cisco SD-WAN Manager, but place the routers in Invalid state so that they cannot establish control plane or data plane connections and cannot receive their configurations from Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
2. Click **WAN Edge List** and click **Upload WAN Edge List**.
3. In the **Upload WAN Edge List** dialog box, choose the file to upload.
4. To upload the router serial number file to Cisco SD-WAN Manager, click **Upload**.

A list of routers in the network is displayed, showing detailed information about each router. To verify that the routers are in the Invalid state, from the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.

Place Routers in Staging State

To move the routers from the Invalid state to the Staging state and then send the serial number file to the controllers, follow the steps below. In the Staging state, the routers can establish control plane connections, over which they receive their configurations from Cisco SD-WAN Manager. However, the routers cannot establish data plane connections.

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. In the **Validate** column, click **Staging** for each router.
4. Click **Send to Controller**.
5. When you are ready to have the router join the data plane in the overlay network, in the **Validate** column, click **Valid** for each router, and then click **Send to Controller**. Placing the routers in the Valid state allows them to establish data plane connections and to communicate with other routers in the overlay network.

Configure the vEdge Routers

Once you have set up and started the virtual machines (VMs) for the vEdge Cloud routers and set up and started the hardware vEdge routers in your overlay network, they come up with a factory-default configuration.

Note **Log In to a Device for the First Time**: When you first deploy a Cisco Catalyst SD-WAN overlay network, log in to the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controller to manually create the device's initial configuration. Routers are shipped with a factory default configuration. If you choose to modify this configuration manually, log in through the router's console port.

For the overlay network to be operational and for the vEdge routers to be able to participate in the overlay network, you must do the following:

- Configure a tunnel interface on at least one interface in VPN 0. This interface must be connected to a WAN transport network that is accessible to all Cisco vEdge devices. VPN 0 carries all control plane traffic between the Cisco vEdge devices in the overlay network.
- Ensure that the Overlay Management Protocol (OMP) is enabled. OMP is the protocol responsible for establishing and maintaining the Cisco Catalyst SD-WAN control plane. It is enabled by default, and you cannot disable it. If you edit the configuration from the CLI, do not remove the **omp** configuration command.
- Ensure that BFD is enabled. BFD is the protocol that the transport tunnels on vEdge routers use for transmitting data traffic through the overlay network. BFD is enabled by default, and cannot be disabled. If you edit the configuration from the CLI, do not remove the **bfd color** command.
- Configure the IP address of DNS name of your network's Cisco SD-WAN Validator.
- Configure the IP address of the router.

Note The DNS cache timeout should be proportional to the number of Cisco SD-WAN Validator IP addresses that DNS has to resolve, otherwise the control connection for Cisco SD-WAN Manager may not occur during a link failure. This is because, when there are more than six IP addresses (this is the recommended number since the default DNS cache timeout is currently two minutes) to be checked, the DNS cache timer expires even as the highest preferred interface tries all Cisco SD-WAN Validator IP addresses, before failing over to a different color. For instance, it takes about 20 seconds to attempt to connect to one IP address. So, if there are eight IP addresses to be resolved, the DNS cache timeout should be 20*8=160 seconds or three minutes.

You should also assign a system IP address to each vEdge router. This address, which is similar to the router ID on non-Cisco vEdge devices, is a persistent address that identifies the router independently of any interface addresses. The system IP is a component of the device's TLOC address. Setting the system IP address for a device allows you to renumber interfaces as needed without affecting the reachability of the Cisco vEdge device. Control traffic over secure DTLS or TLS connections between Cisco SD-WAN Controllers and vEdge routers and between Cisco SD-WAN Controllers and Cisco SD-WAN Validators is sent over the system

interface identified by the system IP address. In the transport VPN (VPN 0), the system IP address is used as the loopback address of the device. You cannot use the same address for another interface in VPN 0.

You can also configure other features and functions required for your network topology.

You configure vEdge routers by creating configuration templates on the Cisco SD-WAN Manager. For each configuration templates, you create one or more feature templates, which you then consolidate into a vEdge router device template. You then attach the device template to a vEdge router. When the vEdge router joins the overlay network, the Cisco SD-WAN Manager automatically pushes the configuration template to the router.

It is strongly recommended that you create the full configuration for vEdge routers by creating configuration templates on the Cisco SD-WAN Manager. When the Cisco SD-WAN Manager discovers a router in the overlay network, it pushes the appropriate configuration template to the device. The configuration parameters in the configuration template overwrite the initial configuration.

Create Configuration Templates for the vEdge Routers

To create vEdge configuration templates, first create feature templates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. In the left pane, select vEdge Cloud or a router model.
5. In the right pane, select the **System feature template**. Configure the following parameters:
   a. Template Name
   b. Description
   c. Site ID
   d. System IP
   e. Timezone
   f. Hostname
   g. Console baud rate (vEdge hardware routers only)
   h. GPS location
6. Click **Save** to save the System template.
7. In the right pane, select **VPN-Interface-Ethernet feature template**. Configure the following parameters:
   a. Template Name
   b. Description
   c. Shutdown No

d. Interface name

e. IPv4 address (static or DHCP)

f. IPv6 address (static of DHCPv6), if desired (in Releases 16.3 and later)

g. Tunnel interface (for VPN 0), color, encapsulation, and services to allow.

8. Click **Save** to save the VPN-Interface Ethernet template.
9. In the right pane, select other templates to configure any desired features. Save each template when you complete the configuration. For information about configuration cellular parameters for vEdge 100m and vEdge 100wm routers, see the next section in this article.

For information about configuration templates and parameters, see the Cisco SD-WAN Manager configuration help articles for your software release.

Next, create a device template that incorporates all the feature templates for the vEdge router:

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down, select the type of device for which you are creating the device template. Cisco SD-WAN Manager displays the feature templates for the device type you selected. Required templates are indicated with an asterisk (*).
5. Enter a name and description for the device template. These fields are mandatory. The template name cannot contain special characters.
6. In the **Transport & Management VPN** section, under VPN 0, from the drop-down list of available templates, select the desired feature template. The list of available templates shows the ones that you have previously created.
7. To include additional feature templates in the device template, in the remaining sections, select the feature templates in turn, and from the drop-down list of available templates, select the desired template. The list of available templates are the ones that you have previously created. Ensure that you select templates for all mandatory feature templates and for any desired optional feature templates.
8. Click **Create** to create the device template.

To attach a device template to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. For the selected template, click **...** and select **Attach Device**.
4. In the **Attach Device** window, either search for a device or select a device from the **Available Device(s)** column.
5. Click the arrow pointing right to move the device to the **Selected Device(s)** column on the right.
6. Click **Attach**.

When Cisco SD-WAN Manager discovers that the vEdge router has joined the overlay network, it pushes the configuration template to the router.

Configuring Cellular Routers

For vEdge 100m and vEdge 100wm routers, you configure cellular interface parameters on the VPN-Interface-Cellular feature template. In this template, the default Profile ID is 0, which enables automatic profile selection. The automatic profile uses the Mobile Country Code/Mobile Network Code (MCC/MNC) values on the router's SIM card. Profile 0 enables the cellular router to automatically join the overlay network during the Cisco Catalyst SD-WAN ZTP automatic provisioning process .

If your MCC/MNC is not supported, the automatic profile selection process fails, and the ZTP process is unable to autodetect the router. In this case, you must configure a cellular profile as follows:

1. In the right pane, select the Cellular Profile feature template.
2. Set the Profile ID to a value from 1 through 15, and configure the desired cellular parameters.
3. Save the Cellular Profile feature template.
4. In the right pane, select the VPN-Interface-Cellular template.
5. Select the Profile ID you configured in Step 2, and for Shutdown, click Yes.
6. Save the VPN-Interface-Cellular feature template.
7. Include the Cellular Profile and VPN-Interface Cellular templates in a device template.
8. Attach the device template to the vEdge router to activate the MCC/MCN.
9. In the right pane, select the VPN-Interface-Cellular template.
10. For Shutdown click No, to enable the cellular interface.
11. Save the VPN-Interface-Cellular feature template.
12. Repush the device template to the vEdge router. This is the device template that you pushed in Step 8.

Configure the vEdge Routers from the CLI

Normally, you create vEdge router configurations using Cisco SD-WAN Manager configuration templates. However, in some situations, such as network test and proof-of-concept (POC) environments, you might want to configure vEdge routers manually, either to speed up the configuration process or because your test environment does not include Cisco SD-WAN Manager. In such situations, you can configure vEdge routers from the router's CLI.

Note If you configure a vEdge router manually from the CLI and then the router later becomes managed by a Cisco SD-WAN Manager, when the Cisco SD-WAN Manager discovers the router, it pushes the router's configuration from the Cisco SD-WAN Manager server to the router, overwriting the existing configuration.

For vEdge Cloud routers, use SSH to open a CLI session to the router. For hardware vEdge routers, connect to the router via the management console.

Configure Minimum Parameters from the CLI

To create the initial configuration on a Cisco vEdge device from a CLI session:

1. Open a CLI session to the Cisco vEdge device via SSH or the console port.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

   ```
   vEdge# config
   vEdge(config)#
   ```

4. Configure the hostname:

   ```
   vEdge(config)# system host-name hostname
   ```

   Configuring the hostname is optional, but is recommended because this name in included as part of the prompt in the CLI and it is used on various Cisco SD-WAN Manager pages to refer to the device.

5. Configure the system IP address. Starting from Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address.

   ```
   vEdge(config-system)#system-ip ip-address
   ```

   Cisco SD-WAN Manager uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the numeric identifier of the site where the device is located:

   ```
   vEdge(config-system)# site-id site-id
   ```

7. Configure the organization name:

   ```
   vEdge(config-system)# organization-name organization-name
   ```

8. Configure the IP address of the Cisco SD-WAN Validator or a DNS name that points to the Cisco SD-WAN Validator. The IP address of the Cisco SD-WAN Validator must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach the Cisco SD-WAN Validator:

   ```
   vEdge(config-system)# vbond (dns-name | ip-address)
   ```

9. Configure a time limit for confirming that a software upgrade is successful:

   ```
   vEdge(config-system)# upgrade-confirm minutes
   ```

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, the Cisco SD-WAN Manager (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not received the confirmation within the configured time, it reverts to the previous software image.

10. Change the password for the user "admin":

```
vEdge(config-system)# user admin password password
```

The default password is "admin".

11. Configure an interface in VPN 0 to be used as a tunnel interface. VPN 0 is the WAN transport VPN, and the tunnel interface carries the control traffic among the devices in the overlay network. For vEdge Cloud routers, the interface name has the format **eth** *number*. For hardware vEdge routers, the interface name has the format **ge** *slot* / *port*. You must enable the interface and configure its IP address, either as a static address or as a dynamically assigned address received from a DHCP server. Starting from Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address, or you can configure both to enable dual-stack operation. In earlier releases, it must be an IPv4 address.

```
vEdge(config)# vpn 0
vEdge(config-vpn-0)# interface interface-name
vEdge(config-interface)# (ip dhcp-client | ip address prefix/length)
vSmart(config-interface)# (ipv6 address ipv6-prefix/length | ipv6 dhcp-client
[dhcp-distance number | dhcp-rapid-commit])
vEdge(config-interface)# no shutdown
vEdge(config-interface)# tunnel-interface
```

Note You must configure a tunnel interface on at least one interface in VPN 0 in order for the overlay network to come up and for the Cisco SD-WAN Manager to be able to participate in the overlay network. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

12. Configure a color for the tunnel to identify the type of WAN transport. You can use the default color (**default**), but you can also configure a more appropriate color, such as **mpls** or **metro-ethernet**, depending on the actual WAN transport.

    vEdge(config-tunnel-interface)# **color** *color*

13. Configure a default route to the WAN transport network:

```
vEdge(config-vpn-0)# ip route 0.0.0.0/0 next-hop
```

14. Commit the configuration:

```
vEdge(config)# commit and-quit
vEdge#
```

15. Verify that the configuration is correct and complete:

```
vEdge# show running-config
```

After the overlay network is up and operational, create a vEdge configuration template on the Cisco SD-WAN Manager that contains the initial configuration parameters. Use the following Cisco SD-WAN Manager feature templates:

- System feature template to configure the hostname, system IP address, and Cisco SD-WAN Validator functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN-Interface-Ethernet feature template to configure the interface in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- From the Cisco SD-WAN Manager menu, select **Administration** > **Settings** and configure Organization name.
- From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates**. For the NTP and System feature configuration templates, configure Timezone, NTP servers, and device physical location.
  - For the Banner feature configuration template, configure Login banner.
  - For the Logging feature configuration template, configure Logging parameters.
  - For the AAA feature configuration template, configure AAA, and RADIUS and TACACS+ servers.
  - For the SNMP feature configuration template, configure SNMP.

Sample Initial CLI Configuration

Below is an example of a simple configuration on a vEdge router. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vEdge# show running-config
system
 host-name         vEdge
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip         172.16.251.20
 site-id           200
 max-controllers   1
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 upgrade-confirm   15
 vbond 184.122.2.2
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 !
 logging
  disk
   enable
  !
 !
 ntp
  keys
   authentication 1 md5 $4$L3rwZmsIic8zj4BgLEFXKw==
   authentication 2 md5 $4$LyLwZmsIif8BvrJgLEFXKw==
   authentication 60124 md5 $4$LXbzZmcKj5Bd+/BgLEFXKw==
   trusted 1 2 60124
  !
```

```
  server 180.20.1.2
   key              1
   source-interface ge0/3
   vpn              1
   version          4
  exit
 !
 radius
  server 180.20.1.2
   vpn              1
   source-interface ge0/3
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
  exit
 !
 tacacs
  server 180.20.1.2
   vpn              1024
   source-interface ge0/3
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
  exit
 !
!

omp
 no shutdown
 gradeful-restart
 advertise bgp
 advertise connected
 advertise static
!
security
 ipsec
  authentication-type ah-sha1-hmac sha1-hman
 !
!
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 community private
  view          v2
  authorization read-only
 !
 trap target vpn 0 10.0.1.1 16662
  group-name     Cisco
  community-name private
 !
 trap group test
  all
   level critical major minor
  exit
 exit
!
vpn 0
 interface ge0/0
  ip address 184.111.20.2/24
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
```

```
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stune
  !
  no shutdown
  bandwidth-upstream   60
  bandwidth-downstream 60
 !
 interface ge0/1
   no shutdown
 !
 interface ge0/2
   no shutdown
 !
 ip route 0.0.0.0/0 184.111.20.1

!
vpn 1
 router
   bgp 111000
    neighbor 172.16.1.20
     no shutdown
     remote-as 111000
     password  $4$LzLwZj1ApK4zj4BgLEFXKw==
    !
   !
   ospf
    timers spf 200 1000 10000
    area 0
     interface ge0/1
       authentication type message-direct
       authentication message-digest message-digest-key 1 md5 $4$LzLwZj1ApK4zj4BgLEFXKw==
      exit
     exit
   !
 !
!
```

Enable Data Stream Collection from a WAN Edge Router

By default, collecting streams of data from a network device is not enabled.

To collect data streams from a WAN Edge router in the overlay network, perform the following steps.

Collecting data streams also requires that VPN 512 be configured in your Cisco Catalyst SD-WAN network.

1. From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.
2. Click **Data Stream**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.1 or earlier, click **Edit**.)
3. Enable **Data Stream**.
4. From Cisco vManage Release 20.4.1, choose one of the following **IP Address Type** options:
   - **Transport**: Click this option send the data stream to the transport IP address of the Cisco SD-WAN Manager node to which the device is connected.
   - **Management**: Click this option send the data stream to the management IP address of the Cisco SD-WAN Manager node to which the device is connected.

- **System**: Click this option to send the data stream to the internally configured system IP address of theCisco SD-WAN Manager node to which the device is connected.

  In a Cisco SD-WAN Manager cluster deployment, we recommend that you choose **System** so that the data stream is collected from edge devices that are managed by all Cisco SD-WAN Manager instances in the cluster.

5. From Cisco vManage Release 20.4.1, perform one of these actions:

   - If you choose **Transport** as the IP address type, in the **Hostname** field, enter the public transports IP address that is used to connect to the router.

     You can determine this IP address by using an SSH client to access the router and entering the **`show interface`** CLI command.

   - If you choose **Management** as the IP address type, in the **Hostname** field, enter the IP address or name of the host to collect the data.

     We recommend that this host is one that is used for out-of-band management and that it is located in the management VPN.

   This **Hostname** option is dimmed when **IP Address Type** is **System**.

6. In the **VPN** field, enter the number of the VPN in which the host is located.

   We recommend that this VPN be the management VPN, which is typically VPN 512.

   This **VPN** option is dimmed when **IP Address Type** is **System**.

7. Click **Save**.

Prepare Routers for ZTP

Cisco Catalyst SD-WAN provides an automatic provisioning software as a service (SaaS) called zero-touch provisioning (ZTP), which allows hardware vEdge routers to join the overlay network automatically. The ZTP process begins when you power on a hardware vEdge router for the first time.

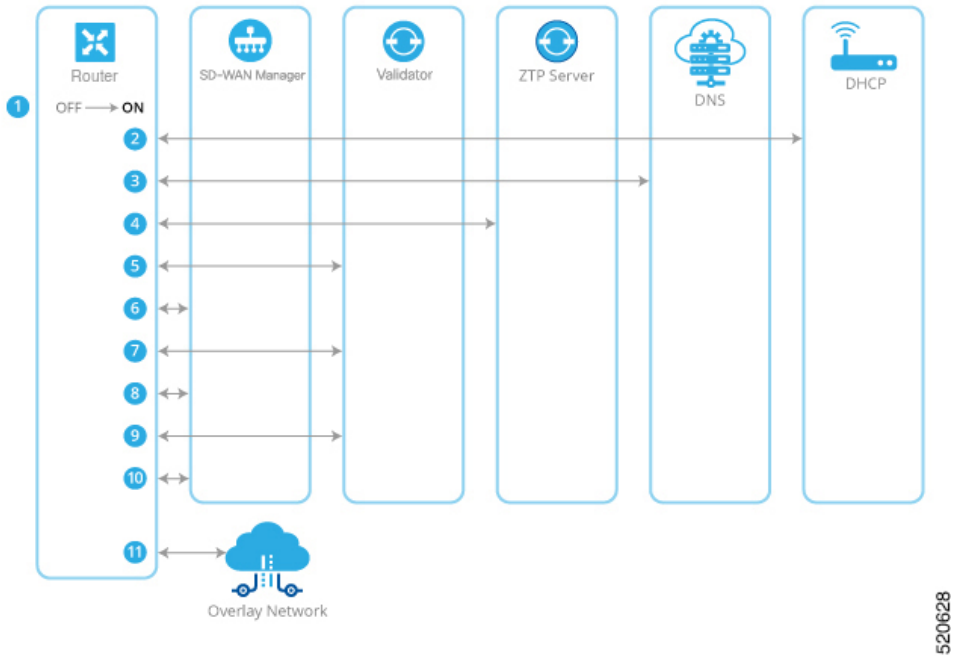
For the ZTP process to work:

- The edge or gateway router at the site where the hardware vEdge router is located must be able to reach public DNS servers. We recommend that the router be configured to reach the Google public DNS servers.
- For Cisco vEdge devices, the edge or gateway router at the site must be able to reachztp.viptela.com.
- For Cisco IOS XE Catalyst SD-WAN devices, the edge or gateway router at the site must be able to reach ztp. *local-domain*.
- A network cable must be plugged into the interface that the hardware router uses for ZTP. These interfaces are:
  - For Cisco vEdge 1000 routers: ge0/0
  - For Cisco vEdge 2000 routers: ge2/0
  - For Cisco vEdge 100 series routers: ge0/4
  - For Cisco IOS XE Catalyst SD-WAN devices, there is no specific interface that is used for connection to the ZTP server. The router attempts to obtain a DHCP IP address on one interface at a time. It

uses the first interface on which it obtains the DHCP IP address to resolve the domain name ztp. *local-domain* to the IP address of the ZTP server.

The ZTP process occurs in the following sequence:

Figure 27: Sequence Flow of the ZTP Process



1. The hardware router powers up.
2. The router attempts to contact a DHCP server, sending a DHCP discovery message.
   a. If a DHCP server is present in the network, the router receives a DHCP offer message that contains the IP address of its ZTP interface. Then, the ZTP process continues with Step 3.
   b. For Cisco vEdge devices, and for Cisco IOS XE Catalyst SD-WAN devices from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if no DHCP server is present, the router does not receive a DHCP offer. In this situation, the router initiates an automatic IP address detection process (also referred to as auto-IP). This process examines the ARP packets on the subnetwork and, from these packets, it infers the IP address of the ZTP interface. Then, the ZTP process continues with Step 3.

      For Cisco IOS XE Catalyst SD-WAN devices before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if no DHCP server is present, the ZTP process does not continue.
3. The router contacts a DNS server to resolve the hostname ztp.viptela.com (for Cisco vEdge devices) or ztp. *local-domain* (Cisco IOS XE Catalyst SD-WAN devices) and receives the IP address of the Cisco Catalyst SD-WAN ZTP server
4. The router connects to the ZTP server. The ZTP server verifies the vEdge router and sends the IP address of the Cisco SD-WAN Validator. This Cisco SD-WAN Validator has the same Organization name as the vEdge router.

5. The router establishes a transient connection to the Cisco SD-WAN Validator and sends its chassis ID and serial number. (At this point in the ZTP process, the router does not have a system IP address, so the connection is established with a null system IP address.) The Cisco SD-WAN Validator uses the chassis ID and serial number to verify the router. The Cisco SD-WAN Validator then sends the IP address of Cisco SD-WAN Manager to the router.
6. The router establishes a connection to and is verified by Cisco SD-WAN Manager. Cisco SD-WAN Manager sends the router its system IP address.
7. The router re-establishes a connection to the Cisco SD-WAN Validator using its system IP address.
8. The router re-establishes a connection to Cisco SD-WAN Manager using its system IP address.

   For Cisco vEdge devices, if necessary, Cisco SD-WAN Manager pushes the proper software image to the vEdge router. As part of the software image installation, the router reboots.
9. After the reboot, the router reestablishes a connection to the Cisco SD-WAN Validator, which again verifies the router.
10. The router establishes a connection to Cisco SD-WAN Manager, which pushes the full configuration to the router. (If the router has rebooted, it re-establishes a connection to Cisco SD-WAN Manager.)
11. The router joins the organization's overlay network.

Note For the ZTP process to succeed, Cisco SD-WAN Manager must contain a device configuration template for the vEdge router. If the Cisco SD-WAN Manager instance has no template, the ZTP process fails. Ignore the device-model and ztp-status display in the configuration preview and intent configuration. This information is visible after you push the configuration on device side.

Using ZTP on Non-Wireless Routers

The default configuration that is shipped on non-wireless hardware vEdge routers includes the following commands that allow the ZTP process to occur automatically:

- **system vbond ztp.viptela.com**—Configures the initial Cisco SD-WAN Validator to be the Cisco Catalyst SD-WAN ZTP SaaS server.
- **vpn 0 interface ip dhcp-client**—Enables DHCP on one of the interfaces in VPN 0, which is the transport interface. Note that the actual interface in the default configuration varies by router model. This interface must be connected to the Internet, MPLS, metro Ethernet, or other WAN network.

Warning: For ZTP to work, do not modify or delete either of these configuration commands before you connect the vEdge router to a WAN.

Using ZTP on Wireless Routers

The vEdge 100m and vEdge 100wm are wireless routers. On these routers, ZTP is supported using both the cellular and the Ethernet interfaces.

Note In Release 16.3, you cannot use the LTE USB dongle on a vEdge 1000 router for ZTP.

The vEdge 100m router supports software Releases 16.1 and later. If the vEdge 100m router is running Release 16.2.10 or later, we recommend, when performing ZTP, that Cisco SD-WAN Manager also be running Release 16.2.10 or later.

The vEdge 100wm router supports software Releases 16.3 and later.

The default configuration that is shipped on wireless hardware vEdge routers includes the following commands that allow the ZTP process to occur automatically on the cellular interface:

- **system vbond ztp.viptela.com**: Configure the initial Cisco SD-WAN Validator to be the Cisco Catalyst SD-WAN ZTP SaaS server.
- **vpn 0 interface cellular0 ip dhcp-client** : Enable DHCP on one of the cellular interface called **cellular0** in VPN 0, which is the transport interface. This interface must be connected to the cellular network.
- **vpn 0 interface cellular0 technology** : Associate a radio access technology (RAT) with the cellular interface. In the default configuration, the RAT is set to **lte**. For ZTP to work, you must change this value to **auto**.
- **vpn 0 interface cellular0 profile 0**: Enable automatic profile selection. For firmware-dependent mobile carriers, the automatic profile uses the firmware default values. For other carriers, the automatic profile uses the Mobile Country Code/Mobile Network Code (MCC/MNC) values on the SIM card. One exception is the vEdge 100m-NT: The automatic profile tries OCN MVNO APN before the firmware default, which is NTT Docomo. If the router finds a matching entry, it autocreates profile 16, which is used for the ZTP connection. To check which profile is being used for the active ZTP connection, look at the Active profile entry in the **show cellular sessions** command output.

  The **profile 0** configuration command recognizes the MCCs and MCNs listed in the vEdge SKU Information table. If your MCC/MNC is supported, you do not need to configure them in the Cellular Profile feature template or with the **profile** command. If your MCC/MNC is not supported, you must configure them manually, using the Cellular-Profile configuration template or the **profile** CLI command.

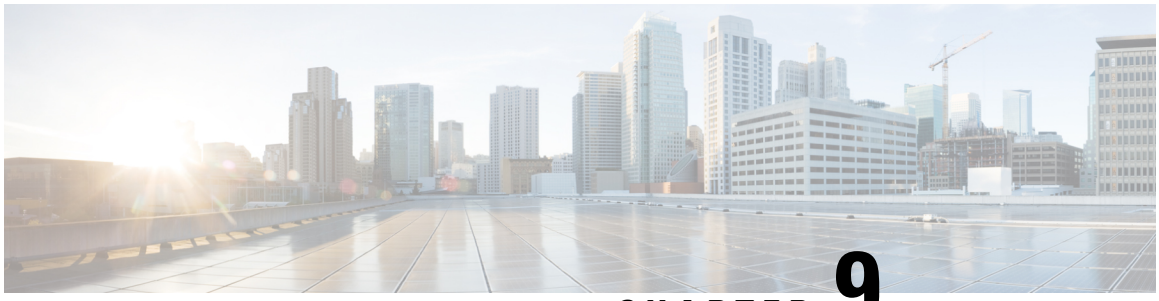
If you need to use Cisco SD-WAN Manager configuration templates to create the portions of the default configuration that allow ZTP to occur automatically, use the VPN-Interface-Cellular feature template. In the template the Profile ID field is set to 0 and the tunnel interface is enabled. Starting from Releases 16.3.1 and later, the Technology field has been added, and the default value is "lte". To match the vEdge router's ZTP cellular0 configuration, change the value to "auto".

Click **Advanced**, to view the default cellular MTU configuration is 1428 bytes:

The following guidelines help to troubleshoot issues that can occur when using ZTP from a wireless router:

- For ZTP to work correctly, ensure that you are using the correct SIM with the correct modem model (SKU).
- If the default profile APN is not configured correctly, the ZTP process does not work correctly. If ZTP does not work, issue the **show cellular status** command to display the error. If an error occurs, configure the appropriate APN and retry the ZTP process.
- For SKUs that do not have default profile APN configurations, such as Generic (MC7304) and North America (MC7354) SKUs, if the automatic profile selection does not detect the APN on the SIM card, configure the profile, including an APN. If the router has a second circuit that has access to Cisco SD-WAN Manager, add the profile information, including the APN, to the feature configuration template and then push the device template to the cellular router. Otherwise, configure the profile on the cellular router from the CLI, including an APN.

- To check whether the router is unable to detect the SIM card, issue the **show cellular status** command. Check for the SIM Read error. To correct this problem, insert the SIM card correctly in the router.
- In Release 16.3.0, after you run ZTP on a cellular router, the cellular interface is in a **no shutdown** state Because of this, Cisco SD-WAN Manager is unable to push a device configuration template to the router. To correct this problem, from the CLI on the router, configure the cellular interface state to be in **shutdown** state.



CHAPTER 9

Add SD-WAN Controller and SD-WAN Validator Components

- Add SD-WAN Controller and SD-WAN Validator components feature history, on page 241
- Add SD-WAN Controller and SD-WAN Validator components, on page 241
- Supported solutions for the Add SD-WAN Controller and SD-WAN Validator workflow, on page 242
- Supported environments for the Add SD-WAN Controller and SD-WAN Validator components workflow, on page 242
- Prerequisites for the Add SD-WAN Controller and SD-WAN Validator components workflow, on page 242
- Add SD-WAN Controllers or SD-WAN Validators using a workflow, on page 242

Add SD-WAN Controller and SD-WAN Validator components feature history

Table 31: Feature history

Feature Name	Release Information	Description
Add Controller and Validator components workflow	Cisco Catalyst SD-WAN Control Components Release 20.18.1	The Add Controller and Validator Components workflow adds these Cisco SD-WAN Control Components to the SD-WAN fabric.

Add SD-WAN Controller and SD-WAN Validator components

The Control Components Certificate Management Workflow in Cisco SD-WAN Manager is a step-by-step interactive procedure (called a workflow) that adds either of these components to an SD-WAN fabric:

- SD-WAN Controller
- SD-WAN Validator

For details about certificate requirements for Cisco SD-WAN Control Components, see *Cisco Catalyst SD-WAN Control Components Certificates and Authorized Serial Number File Prescriptive Deployment Guide*.

Supported solutions for the Add SD-WAN Controller and SD-WAN Validator workflow

The workflow applies to the SD-WAN and SD-Routing solutions.

Supported environments for the Add SD-WAN Controller and SD-WAN Validator components workflow

The workflow is available in Cisco Catalyst SD-WAN environments in which you manage the SD-WAN Control Components.

Prerequisites for the Add SD-WAN Controller and SD-WAN Validator components workflow

Adding these Cisco SD-WAN Control Components requires:

- Management IP address for the SD-WAN Controller or SD-WAN Validator
- Credentials for the SD-WAN Manager that manages the network where you are adding the components
- Certificate file for certificate-based authentication within the Cisco Catalyst SD-WAN environment
- Ability to sign the certificate signing request (CSR) for the certificate

  For signing the certificate, you can choose Cisco-signed or enterprise-signed options.

Add SD-WAN Controllers or SD-WAN Validators using a workflow

Before you begin

See Prerequisites for the Add SD-WAN Controller and SD-WAN Validator components workflow, on page 242.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Launch the Add Controller and Validator Components workflow.

Step 3 Choose either **Controller** or **Validator**, and proceed according to the instructions in the workflow.

For the authentication certificate assigned to the new SD-WAN Control Component, you can do one of these:

- Handle certificate signing within the workflow:
  - Renewal type: Manual

    Choose the option to generate a certificate signing request (CSR). This facilitates getting the certificate signed and ready for use during the workflow. This option provides you with a CSR to download, to get the certificate signed. After getting the certificate signed, you upload the certificate within this workflow.
  - Renewal type: Automatic

    This option is available if two conditions are met:
    - **Administration** > **Settings** > **Certificate setttings** > **Control Components** set to **Cisco**, and
    - Smart Account credentials (**Administration** > **Settings** > **Smart Account Credentials**) are configured.
- Handle certificate signing later:

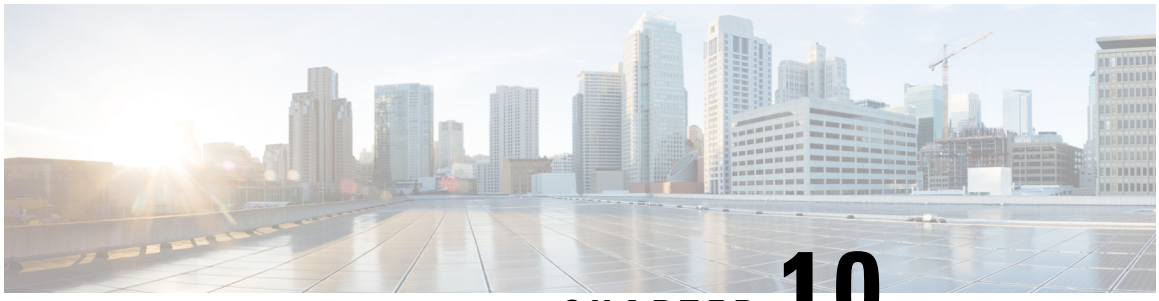
  You can leave the **Generate CSR…** option unselected, and get the certificate signed later. Until the certificate is signed, the new SD-WAN Control Component cannot establish control connections in the network.

The new component appears on the **Configuration** > **Certificates** > **Control Components** page.

What to do next

If you chose to handle certificate signing outside of the workflow, you can handle that using:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **Control Components**.
2. Adjacent to the new SD-WAN Control Component, click **...** > **Generate CSR**.



CHAPTER 10

First Time Settings on Cisco SD-WAN Manager

- First time settings on Cisco SD-WAN Manager, on page 245
- First time settings on Cisco SD-WAN Manager, on page 246
- Standard setup, on page 246
- Express setup, on page 247
- Enable multitenancy on Cisco SD-WAN Manager, on page 247
- Configure organization name, on page 248
- Configure common control component network settings, on page 248
- Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier, on page 258
- Configure cloud services, on page 258
- Configure certificate settings, on page 259
- Add Cisco SD-WAN Controller and Cisco SD-WAN Validator, on page 265
- Configure Cisco SD-WAN Validator IP address, on page 265
- Configure identity provider settings, on page 265
- Configure users and access, on page 266
- Alarm notification settings, on page 267
- Configure account lockout settings, on page 268
- Web server certificate for Cisco SD-WAN Manager, on page 269

First time settings on Cisco SD-WAN Manager

Table 32: Feature History

Feature Name	Release Information	Description
First time Settings on Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature introduces a task flow to setup all the initial settings by a first time user of Cisco SD-WAN Manager.

First time settings on Cisco SD-WAN Manager

When you first use Cisco SD-WAN Manager after onboarding, a guided task flow assists you through the essential configurations. The initial setup guides you through both the mandatory and recommended settings. You have an option to select either a **Standard** or an **Express** setup. Depending on your choice, the setup button appears on the toolbar, allowing you to toggle the task flow open and close.

As you complete a step in the task flow, you can **Mark as complete**. You can choose to **Skip** an optional step or you can choose to **Skip remaining** all the optional steps.

After you configure the mandatory steps, you can stop and restart the task flow at any time. While configuring the optional steps in the task flow, if you navigate to a different screen, use the **Go to this step** option to return to the optional configuration step.

After you update all the basic settings, you can mark the guided task flow as **Complete**. You are automatically navigated to the **Monitor** > **Overview** page.

Standard setup

We recommend that you use the standard setup to complete the initial configurations that are needed to set up the system and onboard network devices.

Table 33: System setup

Setting	Category	On-Prem Deployments	Cloud Deployments
Tenancy mode	Mandatory	Yes	NA
Organization name	Mandatory	Yes	NA
Control component settings	Mandatory	Yes	Yes
Proxy settings	Optional	Yes	Yes
Smart account credentials	Optional	Yes	Yes
Cloud services	Optional	Yes	Yes
Certificate settings	Optional	Yes	Yes
Add control component	Optional	Yes	Yes
Validator address	Optional	Yes	NA

Table 34: Management

Setting	Category	On-Prem Deployments	Cloud Deployments
Identity provider settings	Optional	Yes	Yes

Setting	Category	On-Prem Deployments	Cloud Deployments
Users and access	Optional	Yes	Yes
Alarm notification settings	Optional	Yes	Yes
Account lockout settings	Optional	Yes	Yes
Web server certificate settings	Optional	Yes	Yes

Express setup

In an express setup you can complete the steps that are needed to onboard network devices.

Table 35: System setup

Setting	Category	On-Prem Deployments	Cloud Deployments
Tenancy mode	Mandatory	Yes	NA
Organization name	Mandatory	Yes	NA
Control component settings	Mandatory	Yes	Yes
Proxy setting	Optional	Yes	Yes
Validator address	Optional	Yes	Yes
Certificate settings	Optional	Yes	Yes
Add control component	Optional	Yes	Yes

Enable multitenancy on Cisco SD-WAN Manager

Once multitenancy is enabled on the Cisco SD-WAN Manager, it cannot be migrated back to a single tenant mode.

Procedure

Step 1 Configure the tenancy mode.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Tenancy Mode**.

Step 2 Click **Multitenant**.

Step 3 In the **Domain**, enter the domain name of the service provider (for example, multitenancy.com).

Step 4 Enter a **Cluster Id** (for example, cluster-1 or 123456).

Step 5 Click **Save**.

What to do next

Cisco SD-WAN Manager reboots in multitenant mode and when a provider user logs in to Cisco SD-WAN Manager, the provider dashboard appears.

Configure organization name

Before you can generate a Certificate Signing Request (CSR), you must configure the name of your organization. The organization name is included in the CSR.

Procedure

Step 1 Configure the organization name.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Organization Name**.

Step 2 In **Organization Name**, enter the name of your organization. The organization name must be identical to the name that is configured on the Cisco SD-WAN Validator.

Step 3 In **Confirm Organization Name**, re-enter and confirm your organization name.

Step 4 Click **Save**.

After the control connections are up and running, the organization name bar is no longer editable.

Configure common control component network settings

You can configure common settings or device specific settings for the Cisco SD-WAN Control Components.

Some settings like Banner, Logging and SNMP are disabled by default. You can enable them and then configure the settings.

Procedure

Step 1 Configure common control component network settings

Alternatively, from Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components** and then click **Common control components settings**.

Step 2 Configure the following parameters:

a) Configure NTP

Table 36: NTP

Field	Description
Hostname/IP address	Enter the IP address or FQDN of an NTP server.
VPN ID	Select the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN.
Prefer	Enable if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level.

b) Configure AAA.

Table 37: AAA

Field	Description
Authentication order	From the drop-list choose the authentication order from **local**,**radius**, and **tacacs**.
Cisco TAC enable	For any Cisco SD-WAN Manager troubleshooting issues, enable **Read** and **Write** access.
Click **Add user** and configure the following parameters.	
Username	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommend that you change this password.
User group	Choose the user group from the drop-down menu. You can choose from: • **basic** • **operator** • **netadmin**

Table 38: Advanced

Field	Description
Disable audit logs	Click to disable the audit logs.
Disable netconf logs	Click to disable the netconf logs.
Authentication fallback	Enables authentication fallback.
Admin authentication order	Enables authentication order defined by the administrator.
User accounting	Enables user accounting.
Radius server	
Radius server list	Select the RADIUS server tag from the drop-down menu.
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 5 seconds.
Click **Add server** and configure the following parameters.	
Tag	Enter a value for the server tag.
IP address	Enter the IP address of the RADIUS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 1812
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 through 65535. Default: 1813.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
VPN ID	Select the VPN ID from the drop-down list.

Field	Description
Priority	Set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.
TACACS	
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Authentication	Choose the authentication from the drop-down list.
Click **Add server** and configure the following parameters.	
IP address	Enter the IP address of the TACACS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the TACACS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the TACACS server. Range: 0 through 65535. Default: 49.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS server.
VPN ID	Select the VPN ID from the drop-down list.
Priority	Set the priority of a TACACS server, as a means of choosing or load balancing among multiple TACACS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

c) Configure DNS.

Table 39: DNS

Field	Description
Primary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Secondary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Click **Add host mapping** and configure the following parameters.	
Hostname	Enter the DNS name.
List of IP address	Enter a list of IP addresses seperated by comma.

d) Configure Security.

Table 40: Security

Field	Description
Control connection protocol	Choose the protocol to use on control plane connections: • **DTLS** (Datagram Transport Layer Security). This is the default. • **TLS** (Transport Layer Security)
TLS port	If you select TLS, configure the port number to use: Range: 1025 through 65535. Default: 23456

e) Configure controller.

Table 41: Controller

Field	Description
Graceful Restart for OMP	Enables graceful restart. By default, graceful restart for OMP is enabled.
Graceful Restart Timer (seconds)	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. Range: 0 to 31556952 seconds (365 days) Default: 43200 seconds (12 hours)

Field	Description
Number of Paths Advertised per Prefix	Specify the maximum number of equal-cost routes to advertise per prefix. s advertise routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to eight TLOCs, and by default advertises each route-TLOC tuple to the Cisco Catalyst SD-WAN Controller. If a local site has two Cisco IOS XE Catalyst SD-WAN devices, a Cisco Catalyst SD-WAN Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. Range: 1 to 16 Default: 4
Send Backup Paths	Enable to have OMP advertise backup routes to Cisco IOS XE Catalyst SD-WAN devices. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes.
Shutdown	Ensure that No is chosen to enable to the Cisco SD-WAN overlay network. Click Yes to disable OMP and disable the Cisco SD-WAN overlay network. OMP is enabled by default.
Hub & Spoke Topology	Enable to allow routes through hub and spoke topologies.
Click **Add Compatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.
Click **Add incompatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.

Table 42: Advanced settings

Field	Description
Discard Rejected Routes	Enable to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes aren't discarded.
Enable Filtering Route Updates Based on Affinity	Enable filtering route updates based on affinity.

Field	Description
Enable Filtering Route Updates Based on TLOC-Color	Enable filtering route updates based on TLOC color.
Hold Time (seconds)	Specify how long to wait before closing the OMP connection to a peer. If the peer doesn't receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed. Range: 0 to 65535 seconds Default: • Cisco Catalyst SD-WAN Control Components Release 20.16.x: 5400 seconds • From Cisco Catalyst SD-WAN Control Components Release 20.12.1 to Cisco Catalyst SD-WAN Control Components Release 20.15.x: 300 seconds • Before Cisco Catalyst SD-WAN Control Components Release 20.12.1: 60 seconds
Advertisement Interval (seconds)	Specify the time between OMP Update packets. Range: 0 to 65535 seconds Default: 1 second We recommend you to configure 5 seconds on edge devices and 20 seconds on Cisco SD-WAN Controller.
EOR Timer (Seconds)	Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that weren't refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. Range: 1 to 3600 seconds (1 hour) Default: 300 seconds (5 minutes)

f) Configure banner.

Table 43: Banner

Field	Description
Login message	Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type **\n**.
MOTD message	On a Cisco IOS XE Catalyst SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type **\n**.

g) Configure logging.

Table 44: Logging

Field	Description
Hostname	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages.
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0 and 512

h) Configure SNMP.

Table 45: SNMP

Field	Description
Version	Select SNMP version as v2 or v3.
Name for Device	Enter a name for the device.
Contact person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN device or a Cisco vEdge device. It can be a maximum of 255 characters.
Location of device	Enter a description of the location of the device. It can be a maximum of 255 characters.
Click **Add view** and configure the following parameters.	
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 32 characters. You must add a view name for all views before adding a community.

Field	Description
Object Identifiers	Click **Add OID** and configure the following parameters: • **Object Identifiers**: Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • **Exclude OID**: On/Off—Click Off to include the OID in the view or click On to exclude the OID from the view. To save the object identifiers, click Save. To remove an OID from the list, click the trash can icon next to the entry.
Click **Add group** and configure the following parameters.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Security level	Choose the authentication to use for the group. • **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials. • **auth-priv**: Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password and a privacy and privacy password.
View	Choose an SNMP view that the group can access.
Click **Add user** and configure the following parameters.	
Name	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.
Group	Choose the name of an SNMP group.
Authentication password	Enter the authentication password either in cleartext or as an AES-encrypted key.
Privacy password	Enter the privacy password either in cleartext or as an AES-encrypted key.
Click **Add trap group** and configure the following parameters.	

Field	Description
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Trap Type Modules	Click the group number, and configure the following parameters: In **Severity Levels**, select one or more severity levels for the trap—**critical**, **major**, or **minor**. In **Module Name**, select the type of traps to include in the trap group: • **all**: All trap types. • **app-route**: Traps generated by application-aware routing. • **bfd**: Traps generated by BFD and BFD sessions. • **control**: Traps generated by DTLS and TLS sessions. • **dhcp**: Traps generated by DHCP. • **hardware**: Traps generated by hardware. • **omp**: Traps generated by OMP. • **routing**: Traps generated by BGP, OSPF, and PIM. • **security**: Trap generated by certificates, Cisco Catalyst SD-WAN Controller and vEdge serial number files, and IPsec. • **system**: Traps generated by system-wide functions. • **vpn**: Traps generated by VPN-specific functions, including interfaces and VRRP. • **bridge**: Traps generated to notify about events on a network bridge. • **wwan**: Traps generated from wireless network devices. • **policy**: Traps generated to notify about specific events or errors for policies that are defined for the device.
Click **Add trap target** and configure the following parameters.	
VPN ID	Enter the number of the VPN to use to reach the trap server. The only supported VPN ID's are 0 and 512.
IP address	Enter the IP address of the SNMP server.

Field	Description
UDP port	Enter the UDP port number for connecting to the SNMP server.*Range:* 1 though 65535
Trap group name	Select the name of a trap group that was configured under Group.
User name	Enter the username. The username can be a string from 1 to 32 characters.

Step 3 Click **Save**.

Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier



Note From SD-WAN Manager 20.18.2, register the Plug-and-Play service.

Cisco Smart Account credentials are used for connecting to your smart account. Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to:

- PnP Connect
- Cisco Umbrella portal
- Cisco PKI certificates

Procedure

Step 1 Configure Smart Account credentials.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials**.

Step 2 Enter **Username** and **Password**.

Step 3 Click **Save**.

Configure cloud services

To enable Cisco SD-WAN Analytics and access for AI Assistant, configure Cloud Services settings.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Cloud Services** and enable it.

From Cisco Catalyst SD-WAN Manager Release 20.18.2, after you enable Cloud Services, click **Register** in the **Cisco services onboarding** popup that appears and enter your Smart Account credentials.

Alternatively, from Cisco Catalyst SD-WAN Manager Release 20.18.2, you can authenticate for Cloud Services from the **Cisco services registration** page:

a) From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
b) Open **Cisco services registration**.
c) Select **Cloud Services** and click **Register services**.
d) Enter your Cisco Smart Account or Virtual Account credentials.

Step 3 Enter your Cisco Smart Account credentials in the **User ID** and **Password** fields.

Step 4 (Optional) Enable **Analytics**.

Note
Enable this option only if you have deployed Cisco SD-WAN Analytics, and have confirmed that it is reachable by Cisco SD-WAN Manager.

Step 5 (Optional) Enable **Service Access Authorization**

Step 6 Click **Save**.

Configure certificate settings

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**

Step 2 Choose **Certificate settings** .

a) Configure the control component certificate authorization settings:

Table 46: Control Component Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise**

Field	Description
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

b) Configure the WAN edge cloud certificate authorization settings

Table 47: WAN Edge Cloud Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise** • **Automated (Manager signed)** This option is available only if you are upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

c) Configure the hardware WAN edge certificate authorization settings

Table 48: Hardware WAN Edge Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI (SUDI certificate)** • **Enterprise**
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

d) You can configure the enterprise certificate settings in advance or when you configure the certificate authorization for the control components and the WAN edge devices.

Table 49: Enterprise Certificate Settings

Field	Description
Enrollment protocol type	Choose from one of the following: • **Manual** • **EST** • **SCEP** For EST and SCEP options the route type can be vpn 0 or vpn 512, through which you can allow reachability to the CA server.
If you choose **Manual** configure the following parameters.	
Enterprise root certificate	Choose **Select a file** to upload a root certificate authority file. The uploaded root certificate authority displays in the text box.
If you choose **EST** configure the following parameters.	
URL base	Enter the full EST URL seen on CA server for EST/SCEP certificate authorization server.
(Optional) **Username**	Enter the username for the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Password**	Enter the password to authenticate the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **CA Label**	Enter the CA label for EST CA server. Enter the same details here as per the configurations on the CA server. Use the following format to enter the CA label: • ip-address:port and enter alias, or • host-name:port and enter alias
Root CA certificate	Click **Select a file** to upload the root CA certificate of EST/SCEP CA server. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

Field	Description
Generate EST Client CSR	Enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com
Upload signed certificate file	Optionally, click **Select a file** to upload a signed certificate file. The signed certificate is obtained by signing the EST client CSR manually by CA.
If you choose **SCEP** configure the following parameters.	
URL base	Enter the full SCEP URL as configured on the certificate authorization server. With this url you can call endpoints for certificate enrollment and renewal.
(Optional) **Challenge password**	Enter the password for SCEP CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Root CA fingerprint**	Use the md5 fingerprint of root CA.
Root CA certificate	Click **Select a file** to upload the root CA certificate. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

Step 3 Click **Save** .

Add Cisco SD-WAN Controller and Cisco SD-WAN Validator

Procedure

Step 1 Add Cisco SD-WAN Controller and Cisco SD-WAN Validator.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components**.

Step 2 Click **Add control component**. Follow the on-screen instructions to onboard Cisco SD-WAN Controller and Cisco SD-WAN Validator.

Configure Cisco SD-WAN Validator IP address

Procedure

Step 1 Configure the Cisco SD-WAN Validator IP address.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Validator**.

Step 2 Enter the DNS name that points to the Cisco SD-WAN Validator or the IP address of the Cisco SD-WAN Validator and the port number to use to connect to it.

Step 3 Click **Save**.

Configure identity provider settings

You can configure up to three Identity Provider Settings (IdPs) per tenant and a maximum of three IdPs per provider.

Before you begin

Click **Click here to download the SAML metadata** and save the contents in a text file. This data is used for configuring Okta.

Procedure

Step 1 Enable an identity provider.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Identity Provider Settings**.

Click the toggle button to switch between enabling and disabling IdP settings while retaining the existing configuration.

Step 2 Click **IDP Name** and enter a unique name for your IdP.

Step 3 Click **Domain** and enter a unique domain name for your IdP, for example, okta.com.

If the domain name already exists, Cisco SD-WAN Manager generates an error message.

Step 4 In the **Upload Identity Provider Metadata** section, upload the SAML metadata file you downloaded from your IdP.

Step 5 Click **Save**.

What to do next

After you configure a new IdP name, domain, and sign out of your current Cisco SD-WAN Manager session, you are redirected to a unified SAML login page.

In the unified SAML login page, if you require local authentication, remove the login.html portion of the URL. This redirects you to the local authentication page.

In the unified SAML login page, enter the SSO credentials for your IdP.

Note You are redirected to the unified SAML login page each time you access Cisco SD-WAN Manager after configuring a new IdP name and domain.

Configure users and access

Only a user logged in as the admin user or a user who has write permissions can add, edit, or delete users from Cisco SD-WAN Manager. For more information, see Role Based Access Control.

Procedure

Step 1 Click **Users**.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

a) Click **Add users**
b) Enter **Full name**, **Username**, and **Password**. Re-enter the password once more in **Confirm Password**.
c) Enable the **Remote User** option for remote users. If you enable this option, enter an email for the user.
d) Choose **Roles** and **Scope** for the users.
e) Click **Add**.

Step 2 Click **Roles**.

a) Click **Add Role**.
b) Enter **Custom Role Name**.
c) Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to assign a role.
d) Click **Add**.

Step 3 Click **Scope**.

a) Click **Scope**.
b) Enter **Scope Name** and **Description**.
c) Click **Add Nodes**.
d) Choose the required **Nodes** and click **Save**.
e) (Optional) In the **Associations** pane, click **Add Users** to associate users. Choose the users that you want to add.
f) Click **Save**.

The selected users are associated to a scope.

g) (Optional) In the **Configurations** tab, click **Add Configurations** to add configurations.

Choose the available configurations from the following tabs:

1. Configuration Group
2. Device Template
3. Feature Template
4. Feature Profile
5. Security Policy
6. Localized Policy

h) Click **Save**.

A new scope with nodes, users and required configurations is created.

Alarm notification settings

You can configure Cisco SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

Before you begin

Procedure

Step 1 Configure alarm notifications settings.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Alarm notification settings**.

Step 2 To create alarm notifications, click **here** on-screen.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

Step 3 On the **Alarms notifications** page, a list of configured notifications is displayed in the table. For more information, see Alarm Notifications.

Configure account lockout settings

Procedure

Step 1 Configure account lockout settings.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Account Lockout**.

Step 2 Enable **Inactive days before locked out**.

Step 3 Enable **Inactive days before account locked out**. Enter the number of consecutive inactive days after which Cisco SD-WAN Manager locks out a user.

An inactive day is defined as a day on which a user does not log in to Cisco SD-WAN Manager.

Valid values are 2 through 90.

Step 4 Enter the **Number of failed login attempts before lockout**.

Possible values: 1 through 3600

Default: 3600

Step 5 Enter the **Duration within which the failed attempts are counted (minutes)** during which the system counts consecutive unsuccessful login attempts.

For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Managerlocks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes.

Possibe values: 1 through 60

Default: 60

Step 6 **Cooldown or Lockout period** is enabled by default. If you disable it, an administrator must manually unlock the account of a locked-out user.

This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.

Step 7 In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user.

Possible values: 1 through 60

Default: 15

Web server certificate for Cisco SD-WAN Manager

To establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you must generate a CSR to create a certificate, have it signed by a root CA, and then install it. You must install a separate certificate on each Cisco SD-WAN Manager server in a cluster.

Procedure

Step 1 Configure web server certificate settings.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Web Server Certificate**.

Step 2 Click **CSR**.

Step 3 Enter the **Common Name** with the domain name or IP address of the Cisco SD-WAN Manager server.

For example, the fully-qualified domain name of Cisco SD-WAN Manager could be vmanage.org.local.

Step 4 Enter the **Organizational Unit** name within your organization.

Step 5 Enter the **Organization** name as specified by your root CA.

Step 6 Enter the name of the **City** where your organization is located.

Step 7 Enter the **State** in which your city is located.

Step 8 Enter the **Email** address of the organization.

Step 9 In the **2-Letter Country Code** field, enter the two-letter code for the country in which your state is located.

For example, the two-letter country code for the United States of America is US.

Step 10 In the **Subject Alternative Name(SAN) DNS Names** field, enter the DNS names.

Step 11 In the **Subject Alternative Name (SAN) URIs** field, enter the URIs of resources to which the certificate trust should be extended. If you enter more than one URI, separate each URI with a space or a comma.

Enter each URI in *scheme*:*value* format, where *scheme* is the protocol for accessing the resource and *value* is the resource. For example, `https://example.example.com` or `scp://example.example.com`.

Step 12 Click **Generate** to generate the CSR.

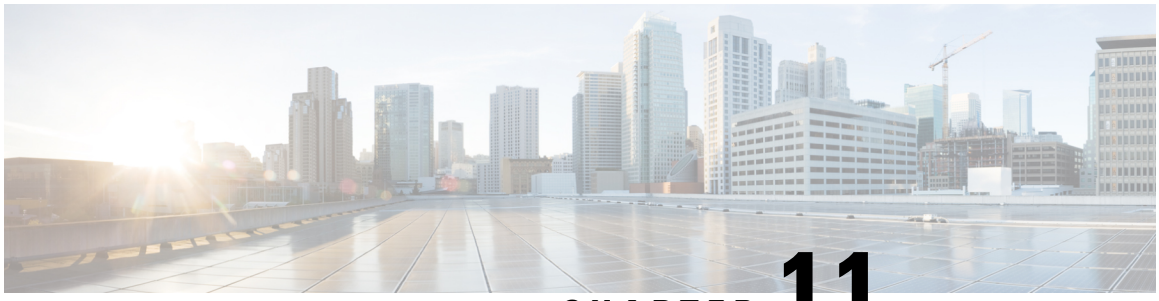
What to do next

Send the CSR to your CA server to have it signed.

When you receive the signed certificate, click **Certificate** in the web server certificate page to install the new certificate. The **View certificate** box displays the current certificate on the Cisco SD-WAN Manager server.

Copy and paste the new certificate in the box. Alternatively, click **Import certificate** and **Select a File** to download the new certificate file.

Restart the application server and log in to Cisco SD-WAN Manager.



CHAPTER 11

Control Components Settings on Cisco SD-WAN Manager

- Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager, on page 271
- Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager, on page 271
- Common Control Component Network Settings, on page 272
- Configure device specific control component network settings, on page 282

Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager

Table 50: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature simplifies the configuration of settings for Cisco SD-WAN Control Components.

Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager

Cisco SD-WAN Manager provides a simplified approach to manage the settings for Cisco SD-WAN Control Components. You can configure common settings or device specific settings for the Cisco SD-WAN Control Components.

To configure the common controller component settings navigate to **Configuration** > **Devices** > **Control Components** and then click **Common control components settings**.

Some settings like **Banner**, **Logging** and **SNMP** are disabled by default. You can enable them and then configure the settings.

The Cisco SD-WAN Control Components configurations can be seen in the column **Managed by**:

- templates, or
- settings.

Each unmanaged Cisco SD-WAN Control Components must be first deployed individually before bulk deploying the settings to all the Cisco SD-WAN Control Components.

To deploy individually to each Cisco SD-WAN Control Components, configure the device specific settings. Click **...** and select **Configure**.

Common Control Component Network Settings

NTP

Click **Add Server** and configure the following parameters.

Table 51: NTP

Field	Description
Hostname/IP address	Enter the IP address or FQDN of an NTP server.
VPN ID	Select the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN.
Prefer	Enable if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level.

AAA

Table 52: AAA

Field	Description
Authentication order	From the drop-list choose the authentication order from **local**,**radius**, and **tacacs**.
Cisco TAC enable	For any Cisco SD-WAN Manager troubleshooting issues, enable **Read** and **Write** access.
Click **Add user** and configure the following parameters.	
Username	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.

Field	Description
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommend that you change this password.
User group	Choose the user group from the drop-down menu. You can choose from: • **basic** • **operator** • **netadmin**

Table 53: Advanced

Field	Description
Disable audit logs	Click to disable the audit logs.
Disable netconf logs	Click to disable the netconf logs.
Authentication fallback	Enables authentication fallback.
Admin authentication order	Enables authentication order defined by the administrator.
User accounting	Enables user accounting.
Radius server	
Radius server list	Select the RADIUS server tag from the drop-down menu.
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 5 seconds.
Click **Add server** and configure the following parameters.	
Tag	Enter a value for the server tag.

Field	Description
IP address	Enter the IP address of the RADIUS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 1812
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 through 65535. Default: 1813.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
VPN ID	Select the VPN ID from the drop-down list.
Priority	Set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.
TACACS	
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Authentication	Choose the authentication from the drop-down list.
Click **Add server** and configure the following parameters.	
IP address	Enter the IP address of the TACACS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the TACACS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49

Field	Description
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the TACACS server. Range: 0 through 65535. Default: 49.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS server.
VPN ID	Select the VPN ID from the drop-down list.
Priority	Set the priority of a TACACS server, as a means of choosing or load balancing among multiple TACACS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

DNS

Table 54: DNS

Field	Description
Primary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Secondary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Click **Add host mapping** and configure the following parameters.	
Hostname	Enter the DNS name.
List of IP address	Enter a list of IP addresses seperated by comma.

Security

Table 55: Security

Field	Description
Control connection protocol	Choose the protocol to use on control plane connections: • **DTLS** (Datagram Transport Layer Security). This is the default. • **TLS** (Transport Layer Security)
TLS port	If you select TLS, configure the port number to use: Range: 1025 through 65535. Default: 23456

Controller

Table 56: Controller

Field	Description
Graceful Restart for OMP	Enables graceful restart. By default, graceful restart for OMP is enabled.
Graceful Restart Timer (seconds)	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. Range: 0 to 31556952 seconds (365 days) Default: 43200 seconds (12 hours)
Number of Paths Advertised per Prefix	Specify the maximum number of equal-cost routes to advertise per prefix. s advertise routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to eight TLOCs, and by default advertises each route-TLOC tuple to the Cisco Catalyst SD-WAN Controller. If a local site has two Cisco IOS XE Catalyst SD-WAN devices, a Cisco Catalyst SD-WAN Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. Range: 1 to 16 Default: 4

Field	Description
Send Backup Paths	Enable to have OMP advertise backup routes to Cisco IOS XE Catalyst SD-WAN devices. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes.
Shutdown	Ensure that No is chosen to enable to the Cisco SD-WAN overlay network. Click Yes to disable OMP and disable the Cisco SD-WAN overlay network. OMP is enabled by default.
Hub & Spoke Topology	Enable to allow routes through hub and spoke topologies.
Click **Add Compatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.
Click **Add incompatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.

Table 57: Advanced settings

Field	Description
Discard Rejected Routes	Enable to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes aren't discarded.
Enable Filtering Route Updates Based on Affinity	Enable filtering route updates based on affinity.
Enable Filtering Route Updates Based on TLOC-Color	Enable filtering route updates based on TLOC color.

Field	Description
Hold Time (seconds)	Specify how long to wait before closing the OMP connection to a peer. If the peer doesn't receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed. Range: 0 to 65535 seconds Default: • Cisco Catalyst SD-WAN Control Components Release 20.16.x: 5400 seconds • From Cisco Catalyst SD-WAN Control Components Release 20.12.1 to Cisco Catalyst SD-WAN Control Components Release 20.15.x: 300 seconds • Before Cisco Catalyst SD-WAN Control Components Release 20.12.1: 60 seconds
Advertisement Interval (seconds)	Specify the time between OMP Update packets. Range: 0 to 65535 seconds Default: 1 second We recommend you to configure 5 seconds on edge devices and 20 seconds on Cisco SD-WAN Controller.
EOR Timer (Seconds)	Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that weren't refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. Range: 1 to 3600 seconds (1 hour) Default: 300 seconds (5 minutes)

Banner

Table 58: Banner

Field	Description
Login message	Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type **\n**.
MOTD message	On a Cisco IOS XE Catalyst SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type **\n**.

Logging

Table 59: Logging

Field	Description
Hostname	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages.
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0 and 512

SNMP

Table 60: SNMP

Field	Description
Version	Select SNMP version as v2 or v3.
Name for Device	Enter a name for the device.
Contact person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN device or a Cisco vEdge device. It can be a maximum of 255 characters.
Location of device	Enter a description of the location of the device. It can be a maximum of 255 characters.
Click **Add view** and configure the following parameters.	
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 32 characters. You must add a view name for all views before adding a community.

Field	Description
Object Identifiers	Click **Add OID** and configure the following parameters: • **Object Identifiers**: Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • **Exclude OID**: On/Off—Click Off to include the OID in the view or click On to exclude the OID from the view. To save the object identifiers, click Save. To remove an OID from the list, click the trash can icon next to the entry.
Click **Add group** and configure the following parameters.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Security level	Choose the authentication to use for the group. • **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials. • **auth-priv**: Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password and a privacy and privacy password.
View	Choose an SNMP view that the group can access.
Click **Add user** and configure the following parameters.	
Name	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.
Group	Choose the name of an SNMP group.
Authentication password	Enter the authentication password either in cleartext or as an AES-encrypted key.

Field	Description
Privacy password	Enter the privacy password either in cleartext or as an AES-encrypted key.
Click **Add trap group** and configure the following parameters.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Trap Type Modules	Click the group number, and configure the following parameters: In **Severity Levels**, select one or more severity levels for the trap—**critical**, **major**, or **minor**. In **Module Name**, select the type of traps to include in the trap group: • **all**: All trap types. • **app-route**: Traps generated by application-aware routing. • **bfd**: Traps generated by BFD and BFD sessions. • **control**: Traps generated by DTLS and TLS sessions. • **dhcp**: Traps generated by DHCP. • **hardware**: Traps generated by hardware. • **omp**: Traps generated by OMP. • **routing**: Traps generated by BGP, OSPF, and PIM. • **security**: Trap generated by certificates, Cisco Catalyst SD-WAN Controller and vEdge serial number files, and IPsec. • **system**: Traps generated by system-wide functions. • **vpn**: Traps generated by VPN-specific functions, including interfaces and VRRP. • **bridge**: Traps generated to notify about events on a network bridge. • **wwan**: Traps generated from wireless network devices. • **policy**: Traps generated to notify about specific events or errors for policies that are defined for the device.

Field	Description
Click **Add trap target** and configure the following parameters.	
VPN ID	Enter the number of the VPN to use to reach the trap server. The only supported VPN ID's are 0 and 512.
IP address	Enter the IP address of the SNMP server.
UDP port	Enter the UDP port number for connecting to the SNMP server.*Range:* 1 though 65535
Trap group name	Select the name of a trap group that was configured under Group.
User name	Enter the username. The username can be a string from 1 to 32 characters.

Configure device specific control component network settings

Load running configuration

When you configure the settings for Cisco SD-WAN Control Components for the first time, Cisco SD-WAN Manager automatically loads the device specific settings from the running configuration of the device. The configurations include system parameters, VPN 0 and VPN 512 static routes, and interface configurations. You can also click **Load running config** to overwrite the existing settings.

System

Field	Description
Hostname	Enter a name for the Cisco Catalyst SD-WAN device. It can be up to 32 characters.
Site ID	Enter the identifier of the site in the Cisco Catalyst SD-WAN overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Cisco Catalyst SD-WAN devices that reside in the same site.*Range:* 1 through 4294967295 ($2^{32} – 1$)
System IP	Enter the system IP address for the Cisco Catalyst SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.

Field	Description
Description	Enter any additional descriptive information about the device.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Timezone	Select the timezone to use on the device.
Latitude	Enter the latitude of the device, in the format *decimal-degrees*.
Longitude	Enter the longitude of the device, in the format *decimal-degrees*.
Device groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Dual stack IPv6 default	This option is available only if you select Cisco SD-WAN Manager and Cisco SD-WAN Controller. Enable to make dual stack IPv6 as the default.
Validator Address	This option is available only if you select Cisco SD-WAN Validator. Enter the IP address of the Cisco SD-WAN Validator.
Controller group ID	This option is available only if you select Cisco SD-WAN Controller. Enter the Cisco SD-WAN Controller groups to which the router belongs.
Overlay ID	This option is available only if you select Cisco SD-WAN Controller. Enter the identifier of the site in the Cisco Catalyst SD-WAN overlay network in which the device resides.
MRF region list	This option is available only if you select Cisco SD-WAN Controller and if you have enabled Multi-Region Fabric. Enter the MRF regions.

VPN and interface

Table 61: VPN 0

Field	Description
Click **Add interface** and configure the following parameters.	

Field	Description
Interface name	Enter a name for the interface. Spell out the interface names completely (for example, eth1). Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.
Shutdown	Enable or disable the interface.
IPv4 type	Configure an IPv4 address assign type. • **Dynamic**: Choose Dynamic to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose Static to enter an IP address that doesn't change. • **None**: Choosing this option means that IPv4 address is not configured.
IPv4 CIDR	Enter an IPv4 address.
IPv4 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IPv6 type	Configure an IPv6 address assign type. • **Dynamic**: Choose Dynamic to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose Static to enter an IP address that doesn't change. • **None**: Choosing this option means that IPv6 address is not configured.
IPv6 CIDR	Enter an IPv6 IP address.
IPv6 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IPv6 DHCP rapid con	Enable DHCP rapid commit, to speed up the assignment of IP addresses.

Field	Description
Tunnel	This option is not available for Cisco SD-WAN Validator. Enable this option to create a tunnel interface.
Tunnel color	Choose a color for the TLOC.
Allow Service	Allow the following services on the interface: • **All** • **DHCP** • **NTP** • **DNS** • **ICMP** • **SSHD** • **STUN** • **NETCONF**

Table 62: IPv4 Static route

Field	Description
Click **Add IPv4 static route** and configure the following parameters.	
IPv4 prefix	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
IPv4 next hop	When you click the next hop, the following fields appear: • **IPv4 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route.

Table 63: IPv6 Static route

Field	Description
Click **Add IPv6 static route** and configure the following parameters.	
IPv6 prefix	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description
IPv6 next hop	When you click the next hop, the following fields appear: • **IPv6 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route.

Table 64: VPN 512

Field	Description
Click **Add interface** and configure the following parameters.	
Interface name	Enter a name for the interface. Spell out the interface names completely (for example, eth1). Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.
Shutdown	Enable or disable the interface.
IPv4 type	Configure an IPv4 VPN interface. • **Dynamic**: Choose Dynamic to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose Static to enter an IP address that doesn't change. • **None**
IPv4 CIDR	Enter an IPv4 IP address.
IPv4 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IPv6 type	
IPv6 CIDR	Enter an IPv6 IP address.
IPv6 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1

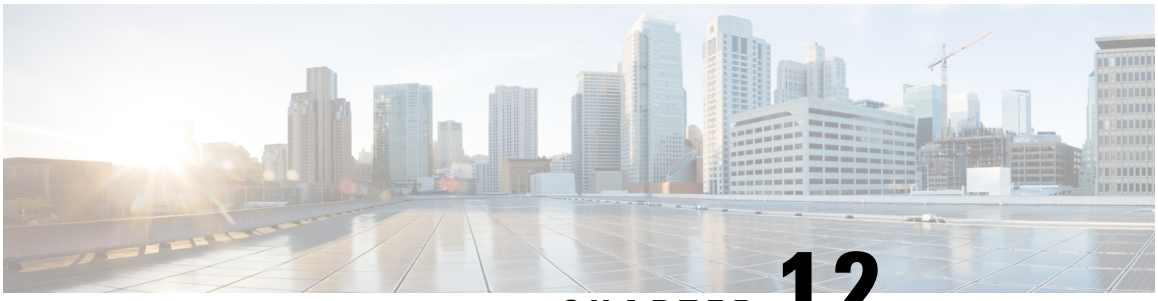
Field	Description
IPv6 DHCP rapid con	Enable DHCP rapid commit, to speed up the assignment of IP addresses.

Table 65: IPv4 Static route

Field	Description
Click **Add IPv4 static route** and configure the following parameters.	
IPv4 prefix	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
IPv4 next hop	When you click the next hop, the following fields appear: • **IPv4 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route. • **None**

Table 66: IPv6 Static route

Field	Description
Click **Add IPv6 static route** and configure the following parameters.	
IPv6 prefix	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.
IPv6 next hop	When you click the next hop, the following fields appear: • **IPv6 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route. • **None**



CHAPTER 12

Cisco SD-WAN Manager Tools

This table describes the developments of this feature, by release.

Table 67: Feature History

Feature Name	Release Information	Description
Global search for Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.18.x	The search box in the SD-WAN Manager header enables you to search for information related to devices, network, and so on. The integration of role-based access control (RBAC) ensures that only authorized users can access data.
TAC case access for AI Assistant in Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.18.2	The AI Assistant now lets you open, view, and close technical assistance center (TAC) cases. **Note** The foundational infrastructure of AI Assistant is included in this release. As a cloud-delivered component of Cisco Catalyst SD-WAN Manager, AI Assistant's capabilities will continue to expand, providing even greater value for customers.

• Cisco SD-WAN Manager header, on page 289

Cisco SD-WAN Manager header

Tools in the Cisco SD-WAN Manager header provide quick access to essential features, including search, the AI Assistant, task management, product help documentation, alarm monitoring, and user profile settings.

Icon	Description
Search	Use the search field to find information on devices, network, configurations, and so on within SD-WAN Manager. SD-WAN Manager maintains search history for each user session. The search results only include information a user is authorized to view, based on role-based access control (RBAC). In a multitenant environment, when a tenant uses the search, SD-WAN Manager returns results related to that tenant only.
AI Assistant	The AI assistant is available in Cisco SD-WAN Cloud and Cloud-Pro installations. It is also available for on-premises customer-hosted SD-WAN deployments that have enabled cloud services and have cloud connectivity.
Tasks	Shows a list of active and completed tasks.
Help	Shows product help, software version, online documentation, and so on. Allows access to Cisco Support Assistant.
Notifications	Shows the details of active and cleared alarms.
User Profile drop-down list	Sign out, or edit your profile.

Cisco Support Assistant

Support Assistant is an in-product support tool that integrates TAC support functions directly into SD-WAN Manager.

To access Support Assistant, select **TAC Support** from the **Help** menu in the header. Support Assistant supports these functions in SD-WAN Manager:

- **Open support case**: Open TAC cases directly from SD-WAN Manager. You can attach relevant logs and files easily, ensuring faster case resolution with minimal manual steps.
- **Record screen**: Record on-screen activities to demonstrate issues visually during case submission. These recordings help TAC engineers quickly understand the problem context for more efficient troubleshooting.
- **Upload local file**: Upload diagnostic files and configuration logs to Cisco TAC. Secure file transfer is integrated directly within SD-WAN Manager. Share your files while maintaining compliance and privacy standards.

For more information on Support Assistant functions, refer to the Cisco Support Assistant website.

Note Support Assistant is enabled when you authenticate within SD-WAN Manager. You need to re-authenticate in each SD-WAN Manager session to use Support Assistant.

AI Assistant

To enable AI Assistant functionality, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and enable **Cloud Services**.

You can access AI Assistant from SD-WAN Manager for various tasks:

- Documentation search. Get information about SD-WAN features and functionalities, such as:
  - What is Cloud OnRamp for SaaS?
  - How do I configure Cloud OnRamp for SaaS?
  - How do I configure Application Aware Routing?
- Monitor and troubleshoot network. Get information about the network and application health, such as:
  - What is the health of my network?
  - Are there any link issues in the last 24 hours?
  - Are there any application performance issues in the last 7 days?



Note To monitor and troubleshoot the network with the AI Assistant, you must enable Cloud Services with Analytics onboarded.

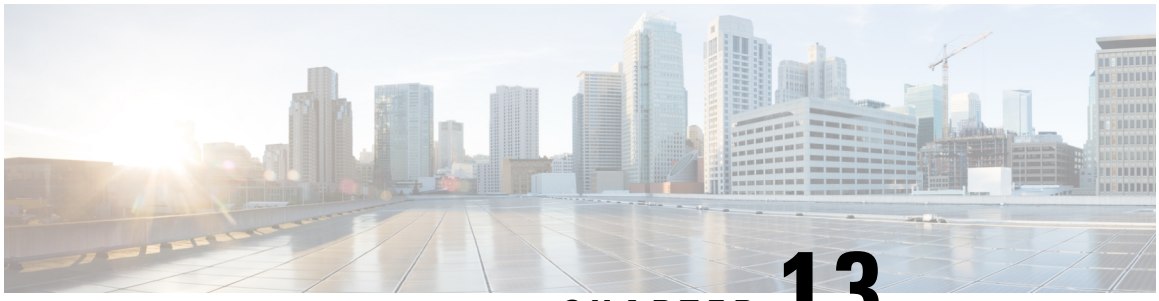
- TAC case management: Open, view, or close a TAC case.

  In order to open a TAC case, you must have a support contract or product under warranty. The cisco.com user account that is used to sign on to Support Case Manager portal must have permission to create, view, and close TAC cases.

  If you provide insufficient information to open a case, the AI assistant provides a TAC portal link with auto-filled information for request completion. You need to complete an authentication workflow for TAC-related actions.



Note Updating or uploading attachment files for existing TAC cases is not supported through the AI Assistant.



CHAPTER 13

Cisco services registration

This table describes the developments of this feature, by release.

Feature Name	Release Information	Description
Authentication for Cisco services	Cisco Catalyst SD-WAN Manager Release 20.18.2	Cisco SD-WAN Manager registers for Cisco services using identity provider-based (IdP) authentication. The Cisco services registration page enables you to register for and authenticate multiple services at once.

- Authentication for Cisco services, on page 293
- Restrictions for authenticating Cisco services , on page 293
- Authenticate Cisco services, on page 294

Authentication for Cisco services

From Cisco Catalyst SD-WAN Manager Release 20.18.2, IdP-based authentication provides a secure method for SD-WAN Manager to authenticate users and obtain access tokens for integrated services. This provides an added layer of security as the credentials are not stored or managed by SD-WAN Manager.

When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.2 from a previous release, ensure to re-register for UTD and License services. You can re-register for other Cisco services if they are currently in use.

Restrictions for authenticating Cisco services

If you have authenticated for a Cisco service and you want to authenticate again using different credentials, your existing browser cookie might contain your previous credentials. In such a case, try one of these:

- Clear the browser cookies.
- Open a window in another browser.
- Open an Incognito tab in the same browser.

Authenticate Cisco services

You can authenticate multiple Cisco services at once with IdP-based authentication from the Cisco services registration page.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Cisco services registration**.

Step 3 Select the services you want to register.

- Single-tenant environment: Cloud Services, Licensing, Plug-n-Play, UTD Snort, and Software Upgrade.
- Service provider in a multitenant environment: Cloud Services, Licensing, Plug-n-Play, UTD Snort, and Software Upgrade.

  Service providers in a multitenant environment and single-tenants from a single-tenant environment are required to register the Plug-n-Play service before:

  - renewing certificates using the Control Components Certificate Management workflow
  - renewing certificates using the edge device certificate management workflow

- Tenant in a multitenant environment: Plug-n-Play and Licensing.

Note
You can also register for UTD Snort by enabling IPS Signatures from the UTD Snort Subscriber Signature.

Step 4 Click **Register services**.

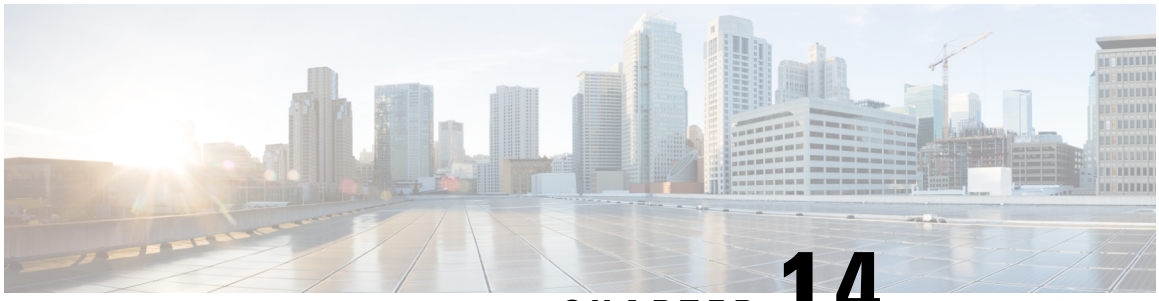
A pop-up window appears with the user code.

Step 5 Click **Next**.

Step 6 Enter your Cisco credentials (Smart Account or Virtual Account credentials).

A success message indicates a successful registration. After registering the services, the table shows the user ID and name corresponding to the credentials you entered, and the date.

To use different credentials for the Smart Account or Virtual Account, use the Quick Connect workflow.



CHAPTER 14

Quick Connect Workflow

- Quick Connect Workflow, on page 295
- Prerequisites for Using the Quick Connect Workflow, on page 296
- Restrictions for Quick Connect Workflow, on page 296
- Information About Quick Connect, on page 297
- Access the Quick Connect Workflow, on page 299

Quick Connect Workflow

Table 68: Feature History

Feature Name	Release Information	Description
Quick Connect Workflow for Onboarding Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides an alternative, guided method in Cisco SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network. As part of the Quick Connect workflow, basic day-0 configuration profiles are created, which apply to all Cisco Catalyst SD-WAN Device (IOS XE) devices, irrespective of the device model and device family. This workflow adds edge devices to the WAN transport and establishes data plane and control plane connections. This feature is supported on Cisco IOS XE Catalyst SD-WAN devices only.

Feature Name	Release Information	Description
Specify a Region and Subregion When Deploying a Device	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	You can specify both a region and a subregion when deploying a device.

Prerequisites for Using the Quick Connect Workflow

- The organization name should be configured.
- Certificate authorization for the Cisco SD-WAN Validator and the Cisco SD-WAN Controller should be configured.
- The controllers (Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller) should be installed and configured.

Note If you haven't configured these, the Quick Connect workflow directs you to the **Administration** > **Settings** window in Cisco SD-WAN Manager to complete the prerequisite configuration.

Restrictions for Quick Connect Workflow

WAN settings

The Quick Connect workflow is limited to configuring WAN settings (VPN 0). To be able to complete the Cisco Catalyst SD-WAN overlay bring up process, you also need to configure service-side VPN templates.

For detailed information about configuring network interfaces, see Configure Network Interfaces.

Platform support

The Quick Connect workflow is supported for Cisco Catalyst SD-WAN Device (IOS XE) devices only.

Single in-progress workflow

You can have only one in-progress workflow at any given point.

Maximum number of devices for the Quick Connect workflow

The Quick Connect workflow supports creating day-0 configurations for a maximum of 500 devices at a time, with these exceptions:

- Cisco Catalyst SD-WAN Manager Release 20.14.1 and 20.16.x: Maximum 25 devices at a time
- Cisco Catalyst SD-WAN Manager Release 20.15.1: Maximum of 25 devices at a time. Later releases of 20.15.x support 500.

If you have more than the maximum number of devices, run the workflow more than once.

Information About Quick Connect

Overview of the Quick Connect workflow

The Quick Connect workflow in Cisco SD-WAN Manager creates a basic day-0 configuration profile, which is applicable to all Cisco IOS XE SD-WAN devices, irrespective of the device family and model. This workflow establishes control plane and data plane access in your WAN.

The behavior of the Quick Connect workflow depends on how you upload devices to Cisco SD-WAN Manager. You can upload your devices in one of the following ways, either as part of the Quick Connect workflow or independently.

- Using the auto sync option, where your Smart Account is synced with Cisco SD-WAN Manager. This option requires Cisco SD-WAN Manager to be able to connect with the Cisco Plug n Play (PnP) portal
- Using the manual upload method, where you download the authorized serial number file of devices from the Cisco PnP portal and upload it to Cisco SD-WAN Manager

IP addresses for onboarded devices

The Quick Connect workflow assigns IP addresses to newly onboarded devices like this:

- It assigns addresses from the system IP pool if
  - you have defined a system IP pool (see Create a system IP pool), and
  - system IP selection is set to Auto in the Quick Connect workflow.
- Otherwise, it uses IP addresses that you enter manually in one of the steps of the workflow.

Upload devices using Auto Sync

From Cisco Catalyst SD-WAN Manager Release 20.18.2, tenants in a single-tenant environment must register the Plug-and-Play service using Smart Account or Virtual Account credentials. When you authenticate the Plug-and-Play service, the devices added to the Cisco PnP portal are auto-synced to Cisco SD-WAN Manager.

The auto sync method of uploading your devices to Cisco SD-WAN Manager can be used for both, deployments that include cloud controllers and deployments that include on-premises controllers, provided that Cisco SD-WAN Manager is able to connect with the Plug n Play (PnP) portal.

How the Auto Sync option works with Cisco PnP, SD-WAN Manager 20.18.1 and earlier

After the Cisco team has configured and deployed the Cisco SD-WAN Controllers, an email, which includes the Cisco SD-WAN Manager information associated with the order is sent. To add devices to the overlay network in such a case, follow these steps:

1. Log in to Cisco SD-WAN Manager using the default credentials (admin/admin).
2. To transfer device information from Cisco PnP portal to Cisco SD-WAN Manager, sync your Smart Account or Virtual account in Cisco SD-WAN Manager. You need Cisco credentials of the Virtual Account

administrator role for this step. For more information about uploading the WAN Edge router serial numbers, see Upload WAN Edge Router Serial Numbers from Cisco Smart Account.

Note Every time you add new devices to the PnP portal, you need to resync Cisco SD-WAN Manager with the Smart Account or the Virtual Account for the new devices to appear in Cisco SD-WAN Manager.

After the device information is transferred to Cisco SD-WAN Manager, you can configure Cisco SD-WAN Manager overlay.

Note For more information about the Cisco PnP portal and its role in onboarding devices for Cisco SD-WAN Manager, see the following reference documentation:

- Cisco Plug and Play Support Guide for Cisco SD-WAN Products
- Plug n Play Onboarding Workflow

How the Auto Sync Option Works with ZTP

If your supported WAN edge devices are registered with Cisco Zero Touch Provisioning (ZTP), the device onboarding is automated and concludes with the devices being authenticated by the Cisco SD-WAN Validator.

With ZTP, after a device is unboxed, connect its WAN port to the network, ensuring that the IP settings from DHCP are configured. This includes configuring the IP address, mask, gateway, and DNS. The device then looks for the ZTP server, which is aware of the Cisco PnP portal inventory. The ZTP server then authenticates the device and redirects it to the Cisco SD-WAN Validator for further authentication.

Note For more information about configuring the vEdge routers to join the overlay network automatically, see Prepare Routers for ZTP.

How Devices Onboarded Using the Auto Sync Option Appear

If you upload devices to Cisco SD-WAN Manager using one of the auto sync options (through Cisco ZTP or Cisco PnP), at the end of the Quick Connect workflow, your devices appear in the Cisco SD-WAN Manager dashboard, accessible from **Monitor** > **Overview**.

Cisco vManage Release 20.6.x and earlier: If you upload devices to Cisco SD-WAN Manager using one of the auto sync options (through Cisco ZTP or Cisco PnP), at the end of the Quick Connect workflow, your devices appear in the Cisco SD-WAN Manager dashboard, accessible from **Dashboard** > **Main Dashboard**.

Upload devices manually

You can choose to upload your devices to Cisco SD-WAN Manager manually, if:

- You don't want to use the auto sync option, which requires you to sync your Smart Account with Cisco SD-WAN Manager

- Your Cisco SD-WAN Manager instance is unable to connect with the Cisco PnP portal

How Manual Upload of Devices Works

Follow this procedure to manually upload your devices to Cisco SD-WAN Manager.

1. Download the authorized serial number file or the provisioning file from the Cisco PnP portal. This file is available in the PnP portal under **Controllers** > **Provisioning File**



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.

2. Transfer the device information to Cisco SD-WAN Manager by manually uploading the authorized serial number file to Cisco SD-WAN Manager. For more information about manually uploading the WAN Edge router serial numbers, see Upload WAN Edge Router Authorized Serial Number File.

Quick Connect Behavior with Manual Upload of Devices

If you upload your devices to Cisco SD-WAN Manager using the manual method, they do not appear in the Cisco SD-WAN Manager dashboard until you deploy them using the CLI bootsrap configuration that the Quick Connect workflow generates.

The bootstrap method helps you onboard a factory-shipped WAN Edge device with the configuration needed to securely deploy it to join the Cisco Catalyst SD-WAN network.



Note For the complete procedure to deploy Cisco Catalyst SD-WAN Device (IOS XE)s using the CLI bootstrap configuration, see On-Site Bootstrap Process for Cisco SD-WAN Devices.

Smart Account and Virtual Account credentials

Change credentials to use for logging in to the Smart Account or Virtual Account:

When you begin the Quick Connect workflow, one of the first steps is to synchronize your device inventory. This requires logging in to the Smart Account or Virtual Account that you are using to manage the Cisco licenses used in the network. These accounts support multiple sets of credentials for different users. You can change the credentials that you use to log in to the Smart Account or Virtual Account using the **Switch account** control.

Access the Quick Connect Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows**.
2. **Start a new Quick Connect workflow:** Under the **Library** area, choose **Quick Connect**.

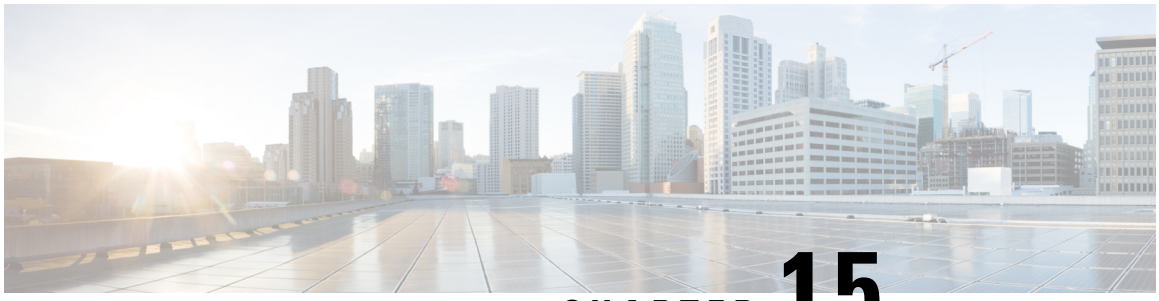
   OR

   Resume an in-progress Quick Connect workflow: Under the **In-progress** area, click **Quick Connect**.

Note If you upload devices to Cisco SD-WAN Manager the manual upload method, you need to complete the additional step of deploying them using the CLI bootstrap configuration that the Quick Connect workflow generates. For more information about generating a bootstrap configuration file that loads to a device, see On-Site Bootstrap Process for Cisco SD-WAN Devices.

Note

- From Cisco Catalyst SD-WAN Manager Release 20.18.2, the **Add and Review Device Configuration** step in the Quick Connect workflow uses the Site Name instead of the Site ID in the Site column. When exporting or importing CSV files, specify the Site Name instead of Site ID, in the Site column.
- From Cisco Catalyst SD-WAN Manager Release 20.18.2, a **Skip configuration** button has been added to the Quick Connect Workflow. This enhancement allows users to directly onboard a device without needing to enter information such as **Hostname**, **System-IP**, or **Site Name**.



CHAPTER 15

Cluster Management

- Cluster Management, on page 301
- Information About Cluster Management, on page 302
- Restrictions for cluster management, on page 302
- Manage the configuration database backup for a Cisco SD-WAN Manager cluster using the CLI, on page 303
- Guidelines for a Cisco Catalyst SD-WAN Manager Cluster, on page 304
- View Available Cluster Services, on page 305
- Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 305
- Add a Cisco Catalyst SD-WAN Manager Server to a Cluster, on page 307
- View Cisco Catalyst SD-WAN Manager Service Details, on page 310
- Edit Cisco Catalyst SD-WAN Manager Parameters, on page 311
- Update Configuration Database Login, on page 311
- Downgrade Cisco Catalyst SD-WAN Manager, on page 313
- Upgrade a Cisco SD-WAN Manager Cluster, on page 313
- Manually Restart Cisco Catalyst SD-WAN Manager Processes, on page 319
- Remove Cisco Catalyst SD-WAN Manager Nodes from a Cluster, on page 321

Cluster Management

Table 69: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Persona-based Cluster Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	Simplifies adding Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

Information About Cluster Management

A Cisco SD-WAN Manager cluster consists of at least three Cisco SD-WAN Manager servers. These servers manage the Cisco Catalyst SD-WAN edge devices in a network. Cisco SD-WAN Manager servers in a cluster perform specific functions based on the services that are running on them. In this way, a cluster distributes the workload among Cisco SD-WAN Manager servers while sharing information between these servers. For scaling recommendations, see *Server Recommendations* for your release in Cisco Catalyst SD-WAN Controller Compatibility Matrix and Server Recommendations.

Use the **Administration** > **Cluster Management** window to create a Cisco SD-WAN Manager cluster and perform related tasks.

From Cisco vManage Release 20.6.1, each Cisco SD-WAN Manager server has a *persona*. The persona is determined when the Cisco SD-WAN Manager server first boots up after Cisco SD-WAN Manager is installed and defines which services run on the server. The persona of a server lasts for the lifetime of the server and cannot be changed. A server must have a persona before it can be added to a cluster. For more information on personas, see Cisco Catalyst SD-WAN Manager Persona and Storage Device.

The role that a server has in a cluster depends on its persona. A Cisco SD-WAN Manager server can have any of the following personas:

- Compute+Data: Includes all services that are required for Cisco SD-WAN Manager, including services that are used for the application, statistics, configuration, messaging, and coordination
- Compute: Includes services that are used for the application, configuration, messaging, and coordination
- Data: Includes services that are used for the application and statistics

Encryption

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, cluster traffic for all services is encrypted.

Reserved IP Addresses

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, a WAN edge device or Cisco SD-WAN Control Components in a Cisco SD-WAN Manager cluster reserve IP addresses with the 172.30.0.0/16 prefix. These reserved IP addresses cannot be used as a system IP address by a WAN edge device or Cisco SD-WAN Control Components. If the reserved IP address is already in use by a WAN edge device or Cisco SD-WAN Control Components, open a TAC case to replace the IP addresses.

Restrictions for cluster management

Describes restrictions, limitations, and important notes regarding cluster management.

Disaster recovery configuration and cluster upgrade by SD-WAN Manager

In a disaster recovery configuration, with active and standby SD-WAN Manager clusters, an SD-WAN Manager instance in the active cluster cannot upgrade nodes in the standby cluster.

Cannot downgrade SD-WAN Control Components

Cisco Catalyst SD-WAN does not support downgrade of SD-WAN Control Components.

Manage the configuration database backup for a Cisco SD-WAN Manager cluster using the CLI

From Cisco Catalyst SD-WAN Control Components Release 20.18.1, you can use CLI commands to manage configuration database backups. These commands allow you to capture a config-db backup, list available backups, download backups, restore backups and add metadata to the config-db backup file.

Procedure

Step 1 Capture a configuration database backup in the online mode.

a) Use this command to generate a config-db backup on demand:

```
request nms configuration-db backup path VM12_Leader_Online
```

The following example demonstrates how to back up the configuration database in the online mode.

```
Device:~# confd_cli
Welcome to Viptela CLI
User root last logged in 2024-05-10T21:11:20.924041+00:00, to vm12, from 127.0.0.1 using cli-console
root connected from 127.0.0.1 using console on vm12
vm12# request nms configuration-db backup path VM12_Leader_Online
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/VM12_Leader_Online.tar.gz
sha256sum: 5c1b0db8518b29c99af856eca0e47f42b262ade13520fbebec7bb9224cebace6
Removing the temp staging dir :/opt/data/backup/staging
Device#
```

Step 2 Capture a configuration database backup in the offline mode.

a) Use the following command to access the internal network namespace:

```
tools internal ip_netns options "exec default bash"
```

b) Dump the configuration database:

Use the following command to dump the configuration database to a .tar.gz file:

```
configuration_db_cmd configuration_db_dump /opt/data/backup/VM12_Leader_Offline.tar.gz
```

This command will create a compressed archive of the database in the specified directory.

The following example demonstrates how to back up the configuration database in the offline mode.

```
vm12# request nms configuration-db stop
Successfully stopped NMS configuration database
vm12# tools internal ip_netns options "exec default bash"
vm12:~# configuration_db_cmd configuration_db_dump /opt/data/backup/VM12_Leader_Offline.tar.gz
Configuration-db dump to /backup/VM12_Leader_Offline.tar.gz
```

Step 3 **View Metadata Information During Restore**

a) Extract the Contents of the Backup File:

Use the following command to extract the contents of the `.tar.gz` file:

```
tar -zxf VM12_Leader_Offline.tar.gz
```

b) View the Metadata Information:

View the contents of the `neo4j_backup_info.json` file:

```
vi neo4j_backup_info.json
```

Note

- The `neo4j_backup_info.json` file contains critical information (metadata) about the backup. Review this information carefully before proceeding with the restore process.

  The metadata includes details such as the backup ID, start time, end time, database version, and system information.

Example

Note The system prompts for confirmation before proceeding with the restore if the backup is older than 24 hours.

Guidelines for a Cisco Catalyst SD-WAN Manager Cluster

The following guidelines apply to a Cisco SD-WAN Manager cluster:

- We recommend that all members of a Cisco SD-WAN Manager cluster be located in the same data center.
- We recommend that the IP addresses of all members of the Cisco SD-WAN Manager cluster be in the same subnet.

Note

- In a multi-node Cisco SD-WAN Manager cluster, the SD-WAN Manager system-ip is the system IP designated by the SD-WAN Manager cluster itself, which may differ from the individual device's system IP.
- The device system-ip is the unique identifier for each device, while the SD-WAN Manager system-ip represents the cluster node managing the control connections.

- We recommend that Cisco SD-WAN Manager cluster interface should not be the same as transport interface. Beginning with Cisco vManage Release 20.9.1, this is enforced. If you attempt to configure this, Cisco SD-WAN Manager displays an error message.
- The cluster interface should not be accessible externally.

- Access to Cisco SD-WAN Manager cluster IP addresses is restricted to Cisco SD-WAN Manager instances in the same cluster.
- The members of a Cisco SD-WAN Manager cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, if you need to change the clock time of a Cisco SD-WAN Manager server in a cluster, make the same change on every Cisco SD-WAN Manager server in the cluster.
- In a three node cluster deployment, only one node can have a systematic failure. When one node fails, the Cisco SD-WAN Manager Graphical User Interface (GUI) of two remaining nodes are reachable and can communicate with remaining nodes through SSH. If two nodes fail, the GUI of an active node on which a user is already logged in allows read-only operations, but new logins to the GUI are not permitted.
- When the guest node has factory default credentials configured on it and a host node tries to add it to the cluster, the cluster management fails. You must modify the password on new node same as that of the other nodes in the cluster.
- When logged in using a single sign-on (SSO) user with netadmin privilege, user cannot perform any of the cluster or disaster recovery operations using the SSO user. For any cluster operations like add, delete node, or enable SD-AVC, Cisco SD-WAN Manager expects any local username and password part of the net-admin group. In case of multitenancy, only admin user can update the SD-AVC. Other users even with netadmin privileges cannot update SD-AVC.
- On devices without dedicated mgmt-intf, VPN 512 gets mapped to custom VRF 512, instead of VRF mgmt-intf. In the back end, this VRF is not mapped to same namespace as other platforms. You cannot download the image as there is a platform difference.
- In clustered environments, when the HTTP proxy is enabled or disabled, restart the application-server on the other nodes for them to pick up latest proxy configuration.

View Available Cluster Services

To view the services that are available in and reachable on all the members in a Cisco SD-WAN Manager cluster, choose **Administration** > **Cluster Management** > **Service Reachability**.

Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server

When you start Cisco SD-WAN Manager for the first time, the default IP address of the Cisco SD-WAN Manager server is shown as localhost. Before you can add a new Cisco SD-WAN Manager server to a cluster, you must change the localhost address of the primary Cisco SD-WAN Manager server to an out-of-band IP address. (From Cisco vManage Release 20.6.1, the primary Cisco SD-WAN Manager server has the Compute+Data persona.) Servers in the cluster use this out-of-band IP address to communicate with each other.

If you need to change the out-of-band IP address in the future, contact your Cisco support representative.

Cluster interconnection between Cisco SD-WAN Manager servers requires that each of the servers be assigned a static IP address. We recommend that you do not use DHCP to assign IP addresses to Cisco SD-WAN

Manager servers that are to be a part of a cluster. Configure the IP address on a nontunnel interface in VPN 0.

Before you configure the cluster IP address of a Cisco SD-WAN Manager server, ensure that out-of-band IP addresses have been configured on VPN0 for its server interfaces. This configuration typically is done when the server is provisioned. The port type for an out-of-band IP address must be **service** for the IP address to be available for assigning to a Cisco SD-WAN Manager server.



Note From Cisco vManage Release 20.11.1, some alarms display the hostname as **localhost** during the cluster setup for the first time as the system-ip/hostname is not configured in Cisco SD-WAN Manager. When the system-ip/hostname is configured, the alarms display the correct hostname.

Configure the IP Address for Releases Before Cisco vManage Release 20.6.1

Configure the IP address of a Cisco SD-WAN Manager server before you add the server to the cluster. To do so for releases before Cisco vManage Release 20.6.1, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add vManage**.

   The **Edit vManage** dialog box opens.
3. From the **vManage IP Address** drop-down list, choose an IP address to assign to the Cisco SD-WAN Manager server.
4. Enter the user name and password for logging in to the Cisco SD-WAN Manager server.
5. Click **Update**.

The Cisco SD-WAN Manager server reboots and displays the **Cluster Management** window.

Configure the IP Address for Cisco vManage Release 20.6.1 and Later Releases

Configure the IP address of a Cisco SD-WAN Manager server before you add the server to the cluster. To do so from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on the primary Cisco SD-WAN Manager server (which has the Compute+Data persona).

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management** window is displayed. The table on this window lists the Cisco SD-WAN Manager servers that are in the cluster.
2. Click **...** adjacent to the Cisco SD-WAN Manager server to configure and click **Edit**.

   The **Edit vManage** dialog box is displayed.
3. In the **Edit vManage** dialog box, perform the following actions.



Note You cannot change the persona of a server. So the Node Persona options are disabled.

a. From the **vManage IP Address** drop-down list, choose an out-of-band static IP address to assign to the server.

b. In the **Username** field, enter the user name for logging in to the server.

c. In the **Password** field, enter the password for logging in to the server.

d. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

   Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on only one Cisco SD-WAN Manager server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.



Note If Cisco SD-WAN Manager is set up as a cluster and the cluster crashes as a result of a reboot or upgrade, the connection to the edge device is reset and the custom app ceases to function.

To resolve this and to resume operation, redefine the custom application name with a new, unique name. For more information to define custom applications, see the Define Custom Applications Using Cisco Catalyst SD-WAN Manager chapter of the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

e. Click **Update**.

   The server reboots and displays the **Cluster Management** window.

Add a Cisco Catalyst SD-WAN Manager Server to a Cluster

Table 70: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Persona-based Cluster Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	Simplifies adding Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

The following sections provide information about adding a Cisco SD-WAN Manager server to a cluster in various Cisco SD-WAN Manager releases.

Add a Cisco SD-WAN Manager Server to a Cluster for Releases Before Cisco vManage Release 20.6.1

To add a new Cisco SD-WAN Manager server to a cluster for releases before Cisco vManage Release 20.6.1, perform the following steps on the primary Cisco SD-WAN Manager server.

Before you begin, ensure that the default IP address of the Cisco SD-WAN Manager server has been changed to an out-of-band IP address as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 305.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add Manager**.

   The **Edit Manager** window opens.
3. In the **Manager IP Address** field, select an IP address to assign to the Cisco SD-WAN Manager server.
4. Enter the username and password for logging in to the Cisco SD-WAN Manager server.
5. Enter the IP address of the Cisco SD-WAN Manager server that you are adding to the cluster.
6. Specify the username and password for the new Cisco SD-WAN Manager server.
7. Select the services to be run on the Cisco SD-WAN Manager server. You can select from the services listed below. Note that the **Application Server** field is not editable. The Cisco SD-WAN Manager Application Server is the local Cisco SD-WAN Manager HTTP web server.
   - Statistics Database: Stores statistics from all the Cisco Catalyst SD-WAN devices in the network.
   - Configuration Database: Stores all the device and feature templates and configurations for all the Cisco Catalyst SD-WAN devices in the network.
   - Messaging Server: Distributes messages and shares state among all the Cisco SD-WAN Manager cluster members.
8. Click **Add**.

   The Cisco SD-WAN Manager server that you just added reboots before joining the cluster.



Note

- In a cluster, we recommend that you run at least three instances of each service.
- When you add the first two compute or compute+data nodes to the cluster, the host node's application-server is unavailable. The following message is displayed on the host node's GUI, before the application-server shuts down in the host node: `\Node added to the cluster. The operation may take up to 30 minutes and may cause application-server to restart in between. Once the application server is back online, the post cluster operation progress can be viewed under tasks pop-up\.`
- Starting Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, ensure that you disable the **HTTP/HTTPs Proxy** option in the Cisco SD-WAN Manager settings, before adding a node to the cluster.

Add a Cisco SD-WAN Manager Server to a Cluster for Cisco vManage Release 20.6.1 and Later Releases

From Cisco vManage Release 20.6.1, a cluster supports any of the following deployments of nodes:

- Three Compute+Data nodes
- Three Compute+Data nodes and three Data nodes

Note DATA nodes should be added only after 3 node cluster with CONFIG+DATA is added.

- Three Compute nodes and three Data nodes (supported only in an upgrade from an existing deployment)

If you require a different combination of nodes, contact your Cisco representative.

To add a Cisco SD-WAN Manager server to a cluster from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on a Compute+Data node or a Compute node. Performing this procedure on a Data node is not supported because a Data node does not run all the services that are required for the addition.

Do not add a server that was a member of the cluster and then removed from the cluster. If you need to add that server to the cluster, bring up a new VM on that server to be used as the node to add.

Before you begin, ensure that the default IP address of the Cisco SD-WAN Manager server has been changed to an out-of-band IP address, as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 305. This operation must happen only once on the Cisco SD-WAN Manager server and then the same is used to add other servers to form a cluster.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management page** window appears. The table on this window shows the Cisco SD-WAN Manager servers that are in the cluster.

2. Click **Add Manager**.

   The **Add Manager** dialog box opens.

Note If the **Edit Manager** dialog box opens, configure an out-of-band IP address for the server, as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 305, and then repeat this procedure for adding a server.

3. In the **Add Manager** dialog box, perform the following actions:

   a. Click the **Node Persona** option (**Compute+Data**, **Compute**, or **Data**) that corresponds to the persona that has been configured for the server.

      You can determine the persona of a server by logging in to the server and looking at the persona display on the **Administration** > **Cluster Management** window. If you choose an incorrect persona, a message displays the persona that you should choose.

   b. From the **Manager IP Address** drop-down list, choose the IP address of the server to be added to the cluster.

   c. In the **Username** field, enter the user name for logging in to the server.

   d. In the **Password** field, enter the password for logging in to the server.

   e. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on one Cisco SD-WAN Manager server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

If you enabled Cisco SD-AVC for this server when you changed its IP address, the **Enable SD-AVC** check box is checked by default.

f. Click **Add**.

g. To confirm, click **OK**.

The dialog box indicates that the services will restart, and that the existing metadata and other information that is not required when the server joins the cluster will be deleted from the server.

When you click **OK**, the system starts the server add operation. The **Cluster Management** window displays the tasks that the system performs as it adds the server.

As part of this operation, the system checks the compatibility of the server that you are adding. This check ensures that the server has sufficient disk space, and that the persona that you specified matches the persona of the node.

After the server is added, the system performs a cluster sync operation, which rebalances the services in the cluster. Then the Cisco SD-WAN Manager servers in the cluster restart.

View Cisco Catalyst SD-WAN Manager Service Details

The following sections describe how to view detailed information about services that are running on a Cisco SD-WAN Manager server and how to view devices that are connected to Cisco SD-WAN Manager.

View Detailed Information about Services

To view detailed information about the services running on a Cisco SD-WAN Manager server:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click the hostname of the Cisco SD-WAN Manager server.

   The **vManage Details** window opens, displaying the process IDs of all the Cisco SD-WAN Manager services that are enabled on Cisco SD-WAN Manager.
3. Click **Cluster Management** in the breadcrumb in the title bar to return to the **Cluster Management** window.

View Devices Connected to Cisco SD-WAN Manager

To view the list of devices connected to Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click the hostname of the Cisco SD-WAN Manager server.
3. Click **Managed Devices**.

Alternatively:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **...** adjacent to the Cisco SD-WAN Manager server and choose **Device Connected**.
3. If a device is connected to Cisco SD-WAN Manager from a cluster, ensure that you do not configure the data stream hostname to the Cisco SD-WAN Manager system IP address. However, you can configure the management IP address on VPN 512 or the internet public IP address on VPN 0. For information about data stream troubleshooting tools, see Data Stream Troubleshooting Tools FAQ.

Edit Cisco Catalyst SD-WAN Manager Parameters

You can edit various parameters for a Cisco SD-WAN Manager server that has been added to a cluster. To do so, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **...** adjacent to the Cisco SD-WAN Manager server to edit, and click **Edit**.

   The **Edit vManage** window opens.
3. Select an IP address to edit.
4. Enter the username and password, and edit parameters for the selected Cisco SD-WAN Manager server.
   - For releases before Cisco vManage Release 20.6.1, you can edit the cluster services.
   - From Cisco vManage Release 20.6.1, you can change the IP address to another IP address that appears in the **vManage IP Address** drop-down list, change the Cisco SD-AVC setting, or change the username and password if the server credentials have changed.
5. Click **Update**.

Update Configuration Database Login

The default username of the configuration database is **neo4j** and the default password is **password**. To update the default login credentials of the configuration database, access Cisco SD-WAN Manager using a terminal and run the following commands. Do not use the SSH terminal option in Cisco SD-WAN Manager to run these commands. Doing so causes you to lose access to Cisco SD-WAN Manager.

1. Use **request nms application-server stop** to stop application servers on all the Cisco SD-WAN Manager servers whether configuration-db is enabled or not.

   .
2. Use one of the following commands to reset the user name and password for the configuration database on all the Cisco SD-WAN Manager servers:
   - For Cisco SD-WAN Release 20.1.1 and earlier:

request nms configuration-db update-admin-user username *username* **password** *password* **newusername** *newadminuser* **newpassword** *newpassword*

- For releases from Cisco SD-WAN Release 20.1.2:

  request nms configuration-db update-admin-user

  When prompted, enter your current username and password, and your new username and password.

  When you run one of these commands, Cisco SD-WAN Manager restarts the application server

Note

- If you do not know the default credentials of the configuration database, contact your Cisco support representative to retrieve the credentials.
- You cannot use a previous username.
- The Cisco SD-WAN Manager configuration-db usernames and passwords must have only the following characters: A-Z, a-z, 0-9, _, -, ., @, and %.
- The usernames and passwords must not begin with a hyphen (-).
- The password must contain at least 8 characters.

Example

- For Cisco SD-WAN Release 20.1.1 and earlier:

```
request nms configuration-db update-admin-user username neo4j
password ******** newusername myusername newpassword mypassword
```

- For releases from Cisco SD-WAN Release 20.1.2:

```
request nms configuration-db update-admin-user
Enter current user name: neo4j
Enter current user password: password
Enter new user name: myusername
Enter new user password: mypassword
```

Note After a configuration database admin user update, if you are unable to view a specific Cisco SD-WAN Manager instance, use the **request nms application-server restart** command to restart the application server on that Cisco SD-WAN Manager instance again.

Note Starting from Cisco SD-WAN Release 20.6.1, when using the **request nms configuration-db update-admin-user** command to update the admin user credentials, provide the same inputs (old username, password and the new username, password) across all the nodes in the Cisco SD-WAN Manager cluster. You must execute the **request nms configuration-db update-admin-user** command one node at a time. We recommend that you do not push the CLI to all the nodes at the same time because the NMS services will restart for the new configuration to take effect.

Downgrade Cisco Catalyst SD-WAN Manager

You cannot downgrade Cisco SD-WAN Manager (install a version of Cisco SD-WAN Manager that is lower than the current version), either through Cisco SD-WAN Manager or by using CLI commands.

Note This restriction applies for single Cisco SD-WAN Manager instances and for Cisco SD-WAN Manager clusters. This restriction is not related to software upgrades or downgrades on network devices.

To downgrade your Cisco SD-WAN Manager version, contact your Cisco support representative.

Upgrade a Cisco SD-WAN Manager Cluster

Table 71: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Cluster Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature outlines the upgrade procedure for Cisco SD-WAN Manager servers in a cluster.
Check for Database Schema Violation	Cisco Catalyst SD-WAN Manager Release 20.13.1	Updated the **request nms application-server status** command to indicate whether there is a schema violation in the configuration database. You can check for violations before upgrading a cluster.

Feature Name	Release Information	Description
Cisco SD-WAN Manager Cluster Upgrade Compatibility Check	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature helps to upgrade a Cisco SD-WAN Manager cluster, performing a pre-upgrade software compatibility check and a post-upgrade check to ensure a successful upgrade. The feature helps to ensure a successful upgrade and helps to troubleshoot any problems in case of an unsuccessful upgrade.

Information About Cluster Upgrade

This section describes how to upgrade Cisco SD-WAN Manager in a cluster.

You can upgrade directly from Cisco vManage 20.3.1 or later releases to Cisco vManage Release 20.6.1. To upgrade from earlier releases, first upgrade to Cisco vManage 20.4.2 or Cisco vManage Release 20.5.1.

If you are upgrading a Cisco SD-WAN Manager cluster deployment from Cisco vManage Release 20.3.1 or later to Cisco vManage Release 20.5.1 or later, you must do it through the CLI.

If you are upgrading to Cisco vManage Release 20.6.1 or later releases from a six-node Cisco SD-WAN Manager cluster deployment in which not all services are running on all nodes, contact your Cisco support representative before performing the upgrade.

Starting with Cisco vManage Release 20.6.1, 6-node cluster deployments support only 3 Compute+Data nodes and 3 Data nodes. If your 6-node cluster is still configured with 3 Compute nodes and 3 Data nodes, **contact your Cisco support representative for assistance** in migrating it to 3 Compute+Data nodes and 3 Data nodes before performing any further upgrades.

Checking Software Compatibility Before Upgrade

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

In a cluster deployment, Cisco SD-WAN Manager services such as the configuration database, coordination service, and messaging services operate in a cluster mode.

Cisco SD-WAN Manager performs an important pre-upgrade check before proceeding with an upgrade. The pre-upgrade check includes items such as certificate expiration dates, the configuration database, CPU, disk, memory, and the status of services such as the coordination service and messaging service. If the cluster is not ready for upgrade, Cisco SD-WAN Manager notifies you.

Check the Cisco Catalyst SD-WAN Upgrade Matrix for information about upgrading.

Cisco SD-WAN Manager performs an important pre-upgrade check before proceeding with an upgrade. The pre-upgrade check includes items such as certificate expiration dates, the configuration database, CPU, disk, memory, and the status of services such as the coordination service and messaging service. If the cluster is not ready for upgrade, Cisco SD-WAN Manager notifies you.

After an upgrade, Cisco SD-WAN Manager performs a post-upgrade check, which includes checking the functionality of services to ensure a successful upgrade. If an upgrade fails, you can use Cisco SD-WAN Manager to troubleshoot and run the upgrade again.

While a cluster upgrade is in progress, at a given time, some nodes in the cluster continue to run an older software release while others have been upgraded to the newer release. Consequently, during the upgrade, there may be incompatibilities between services of the older and newer releases, preventing them from functioning properly.

For information about how to upgrade Cisco SD-WAN Manager clusters using Cisco SD-WAN Manager, see the Software Upgrade section in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide.*

Encryption

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1

For a multitenant cluster upgrade from Cisco Catalyst SD-WAN Manager Release 20.13.1 to Cisco Catalyst SD-WAN Manager Release 20.14.1 using Cisco SD-WAN Manager, the upgrade coordinator sometimes fails due to the encryption keys. The upgrade coordinator service uses the encryption keys to encrypt the service credentials.

To re-encrypt the service credentials, reboot the Cisco SD-WAN Manager and trigger the software activation.

Prerequisites for Cluster Upgrade

Before you upgrade Cisco SD-WAN Manager nodes to Cisco vManage Release 20.6.1 or later releases, verify the following:

- Ensure that the internal user account vmanage-admin is not locked for any server that you are upgrading.

  You can check the status of this admin account by pushing a template to the devices that are connected to the server. The push fails if the account is locked. In such a scenario, you can unlock the account by using the **request aaa unlock-user vmanage-admin** command.

- Ensure that PKI keys have been exchanged between the servers that you are upgrading.

  To do so, ensure that the control connections are in the UP state on the servers and restart the application server.

- Ensure that the out-of-band IP address of each server is reachable.

- Ensure that the Cisco SD-WAN Manager is accessible on all servers in the cluster.

- Ensure that DCA is running on all nodes in the cluster.

  To do so, use the **request nms data-collection-agent status** command and ensure that the status value shows **running** for each node.

  To start DCA, if needed, use the **request nms data-collection-agent start** command.

- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Use the **request nms application-server status** command to verify that there is no schema violation in the configuration database. If the command output indicates a violation, contact Cisco Customer Support to resolve the issue.

- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.3, the compute and data check is a prerequisite for disaster recovery (DR) replications to work. DR is not supported, if you run three compute nodes and three data nodes for DR replication.

If these prerequisites are not met or if another error occurs during the upgrade the activation of the image fails and a file named upgrade-context.json is created in the /opt/data/extra-packages/*image-version* folder on each

node in the cluster. You can provide this file to your Cisco representative for assistance with resolving the issue.

Note In certain cases, the existing data-collection-agent container may remain in the Created state without being removed when a new container is launched. However, only one container with the intended name will be active at any given time. Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the data-collection-agent (DCA) runs as a host service instead of a container, which prevents this behavior.

Upgrade cluster software using SD-WAN Manager

This procedure upgrades the Cisco Catalyst SD-WAN software for an SD-WAN Manager cluster. It uses SD-WAN Manager itself to perform the upgrade. Alternatively, you can use a CLI command procedure to perform the upgrade.

This procedure applies to Cisco Catalyst SD-WAN Control Components Release 20.15.x and later.

Note If the cluster upgrade fails and you cannot log in to SD-WAN Manager, you can roll back to a snapshot taken before upgrading the cluster.

Before you begin

Download the software package for the new software version.

Procedure

Step 1 Upload the new software package.

a) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**, and select the **Software Images** tab.

b) Upload the new software package to the SD-WAN Manager software repository, and confirm that it appears in the table of software images.

Step 2 Upgrade the software for the cluster.

a) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**, and select the **Manager** tab.

The SD-WAN Manager instances in the cluster appear in the table. Depending on your cluster, there will be three or six instances.

b) Select the **Software Image Actions** menu and choose **Upgrade**.

c) In the **Software Upgrade** pane, select **Manager** and choose a software version from the menu.

d) Select **Upgrade**.

Each SD-WAN Manager node in the cluster enters a Scheduled status. The **Status** column in the table shows this. As SD-WAN Manager performs the upgrade on each node, its status changes to In progress.

For details about the progress, you can view the logs for a node by selecting the button in the **Action** column for the node.

When the upgrade is complete for a node, its status changes to Success.

e) Select the **Software Image Actions** menu and select **Activate**.
f) In the **Activate Software** pop-up window, select the version to activate.

Activating the software causes the node to reboot. Rebooting the node logs out all active clients and disconnects the node's control connections.

Each SD-WAN Manager node in the cluster enters a Scheduled status. The **Status** column in the table shows this.

Each node performs prechecks, and then proceeds with activation. As each node activates the new software, its status changes to In progress.

The SD-WAN Manager instance in which you are initiating the upgrade closes and after several minutes shows a system reboot message.

Step 3 Confirm the readiness of the nodes in the cluster.

a) From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** > **Service Configuration**, and confirm that for each node, the **Configure Status** column shows Ready.
b) From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** > **Service Reachability**, and confirm that for each node, the **Application Server** column shows Reachable.

Step 4 Set the newly upgraded software version as the default.

a) From the Cisco SD-WAN Manager menu, open **Maintenance** > **Software Upgrade**, and select the **Control Components** tab.
b) From the **Software Image Actions** menu, select **Set Default Version**.
c) Choose the software release that you have just upgraded to.
d) Select **Set Default**.

It may take several minutes for each node in the cluster to set the new software release as its default.

Upgrade a Cluster Using CLI

1. Take snapshots of all the Cisco SD-WAN Manager servers. Take a backup of the configuration database and save it in a location outside of the Cisco SD-WAN Manager server using the following command:

   request nms configuration-db backup path *path_and_filename*
2. Ensure that Cisco vManage Release 18.3 or later is installed.
3. For upgrades from Cisco vManage Release 20.3.1 or later, copy the current image to each Cisco SD-WAN Manager server in the cluster and install the image on each Cisco SD-WAN Manager server by using the following command. Do not activate the image at this time.

   request software install *path*



Note The copy to Cisco SD-WAN Manager can be done using SCP using CLI using the VPN 512 interface.

4. For upgrades from Cisco vManage Release 20.3.1 or later, activate the current image on each Cisco SD-WAN Manager server using the following command. All servers reboot simultaneously.

request software activate *version*

5. You must upgrade the configuration database when upgrading from one of the following:
   - Cisco vManage Release 18.4.x or 19.2.x to Cisco vManage 20.3.x or 20.4.x
   - Cisco vManage Release 20.3.x or 20.4.x to Cisco vManage Release 20.5.x or 20.6.x
   - Any Cisco SD-WAN Manager release to Cisco vManage Release 20.10.1 or later



Note
- Starting from Cisco vManage Release 20.1.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command:

  request nms *configuration-db diagnostics*
- When you upgrade the configuration database, ensure that you have activated the current image on each Cisco SD-WAN Manager server in the cluster as described in the previous step. In addition, ensure that all services except the application server and configuration-db services are running on these servers by entering the **request nms all status** command on each server.

To upgrade the configuration database, do the following:

a. To determine which node to upgrade, enter the **request nms configuration-db status** command on each node. In the output look for the following:

```
Enabled: true
Status: not running
```



Note After activating a new image on a Cisco SD-WAN Manager host server, the server reboots. After the reboot, for approximately 30 minutes, the output of the **request nms configuration-db status** command shows **Enabled: false** even on a node that has the configuration database enabled, while NMS services are being migrated to a containerized form.

b. If you are upgrading from vManage 20.4.x or earlier, then on the node to upgrade, as determined in the previous step, enter this:

   request nms configuration-db upgrade



Note
- Enter this command on one node only.
- Check the Cisco Catalyst SD-WAN Upgrade Matrix for information about upgrading from vManage 20.5.x or later.

6. Enter your login credentials, if prompted. Login credentials are prompted in releases earlier than Cisco vManage Release 20.3.1 if all the Cisco SD-WAN Manager servers establish control connection with each other. After a successful upgrade, all the configuration database services are UP across the cluster, and the application server is started.

You can check the database upgrade logs at the following location: *vmanage-server*:/var/log/nms/neo4j-upgrade.log.

Manually Restart Cisco Catalyst SD-WAN Manager Processes

If the cluster is malfunctioning and requires restart, you can manually restart the Cisco SD-WAN Manager processes. Do one of the following:

• (Cisco vManage Release 20.6.1 and later) Use the request nms all restart command to restart all processes.

• (Releases earlier than Cisco vManage Release 20.6.1) Restart the processes one at a time in an orderly manner using the procedure that follows. The manual restart order may vary for your cluster, depending on what services you are running on the Cisco SD-WAN Manager instances in the cluster. The following order is based on a basic cluster with three Cisco SD-WAN Manager devices.



Note It is not recommended to restart the NMS services immediately after the software upgrade. You must wait for at least 45 minutes. Beginning with Cisco vManage Release 20.9.1, you can check the status of the NMS service containers using the command **docker ps-a** in the root shell of Cisco SD-WAN Manager before restarting the NMS services. You can contact Cisco TAC for assistance.

1. On each Cisco SD-WAN Manager device, stop all the NMS services:

   ```
   request nms all stop
   ```

2. Verify that all the services have stopped. It is normal for the **request nms all stop** command to display a message about failing to stop a service if it takes too long. So use the following command to verify that everything is stopped before proceeding further:

   ```
   request nms all status
   ```

3. Start the Statistics database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms statistics-db start
   ```

4. Verify that the service is started before proceeding to start it on the next Cisco SD-WAN Manager. After the service starts, perform step 3 to start the Statistics database on the next Cisco SD-WAN Manager device. After all the Cisco SD-WAN Manager devices have the Statistics database running, proceed to the next step.

   ```
   request nms statistics-db status
   ```

5. Start the Configuration database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms configuration-db start
   ```

6. For releases earlier than Cisco vManage Release 20.3.1, verify that the service has started before proceeding to start it on the next Cisco SD-WAN Manager device. Go to vshell and tail a log file to look for a message that the database is online. After confirming, go to step 5 to start the Configuration database on the next Cisco SD-WAN Manager device. After all the Cisco SD-WAN Manager devices have the Configuration database running, proceed to the next step.

   ```
   tail -f -n 100 /var/log/nms/vmanage-neo4j-out.log
   ```

7. Start the Coordination server on each device. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms coordination-server start
   ```

8. Verify that the service is started before proceeding to start it on the next Cisco SD-WAN Manager device. After verifying, go to step 7 to start the Coordination server on the next Cisco SD-WAN Manager device. After the Coordination server runs on all the Cisco SD-WAN Manager devices, proceed to the next step.

   ```
   request nms coordination-server status
   ```

9. Start the Messaging server on each device. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms messaging-server start
   ```

10. Verify that the service has started before proceeding to start the service on the next Cisco SD-WAN Manager device. After verifying, go to step 9 to start the Messaging server on the next Cisco SD-WAN Manager device. After the Messaging server runs on all the Cisco SD-WAN Manager devices, proceed to the next step.

    ```
    request nms messaging-server status
    ```

11. Start the Application server on each device. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

    ```
    request nms application-server start
    ```

12. For Cisco vManage Release 20.3.1 and later releases, start the server-proxy service on each Cisco SD-WAN Manager device:

    ```
    request nms server-proxy start
    ```

    To verify that the service is fully started, open the GUI of that Cisco SD-WAN Manager device. After the GUI is fully loaded and you are able to log in, start the server-proxy service on the next Cisco SD-WAN Manager device.

13. Restart the NMS cloud services on each device. Wait for the services to start each time before proceeding to the next Cisco SD-WAN Manager device.

    You can verify that the cloud services are running by entering the following commands:

    ```
    request nms cloud-agent status
    ```

    ```
    request nms cloud-agent-v2 status
    ```

    Verify that the service has started before proceeding to start it on the next Cisco SD-WAN Manager device. After verifying, start the cloud services on the next Cisco SD-WAN Manager device. After the cloud services run on all the Cisco SD-WAN Manager devices, continue to the next step.

14. To verify that there are no errors and everything has loaded cleanly, tail the log files.

If you experience issues when upgrading to Cisco vManage Release 20.6.1 or later, contact your Cisco support representative for assistance.



Note Consider bringing up the services manually as described in this section whenever you have to reboot a Cisco SD-WAN Manager device, or after an upgrade.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, a **device-data-collector** service container is added. The following is a sample output for the command, **request nms device-data-collector**.

```
Device# request nms device-data-collector
Possible completions:
  diagnostics   Run diagnostics on NMS component
  jcmd          Run jcmd on NMS component
  restart       Restart NMS component
  start         Start NMS component
  status        Status of NMS component
  stop          Stop NMS component
```

Remove Cisco Catalyst SD-WAN Manager Nodes from a Cluster

You can remove a Cisco SD-WAN Manager node from a cluster, if necessary.

In releases earlier than Cisco vManage Release 20.6.1, you can only remove *n* - 2 Cisco SD-WAN Manager nodes from a cluster of *n* nodes. You must retain at least two Cisco SD-WAN Manager nodes in a cluster.

From Cisco vManage Release 20.6.1, you must retain at least two Cisco SD-WAN Manager nodes that include the compute capability and at least one node that includes the data capability. That is, the cluster must retain any of the following:

- At least two Cisco SD-WAN Manager nodes that include the Compute+Data persona
- At least one Cisco SD-WAN Manager nodes that includes the Compute+Data persona and one Cisco SD-WAN Manager node that includes the Compute persona
- At least two Cisco SD-WAN Manager nodes that include the Compute persona and one Cisco SD-WAN Manager node that includes the Data persona

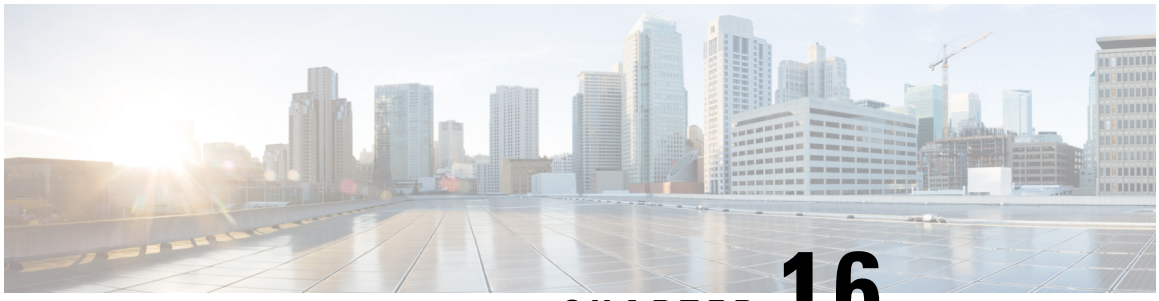
From Cisco vManage Release 20.6.1, if a Cisco SD-WAN Manager node is reachable when you remove it from a cluster, Cisco SD-WAN Manager automatically performs a factory reset operation on the removed node to ensure that the node does not join the cluster again. If a Cisco SD-WAN Manager node is unreachable when you remove it from a cluster, a factory reset operation is not performed on the node. In this situation, the node is added back to the cluster automatically when the node becomes reachable. To prevent the node from being added back to the cluster, enter the command **request software reset** from the CLI of the node after the node is removed from the cluster.

To remove a Cisco SD-WAN Manager node from a cluster, follow these steps:

1. From the Cisco SD-WAN Manager, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **…** adjacent to the Cisco SD-WAN Manager instance that you want to remove and click **Remove**.

   The **Remove Manager** dialog box opens.
3. Enter the username and password to confirm the removal of the device from the network.
4. Click **Remove**.

The Cisco SD-WAN Manager instance is removed from the cluster, the certificates for that Cisco SD-WAN Manager are deleted, and Cisco SD-WAN Manager undergoes a factory reset.



CHAPTER 16

Automated Certificate Management

- Feature history for automated certificate management, on page 323
- Automated certificate management, on page 323
- Prerequisites for automated certificate management on CA servers, on page 324
- Configure certificate settings, on page 325
- Troubleshoot certificate management on CA server, on page 331

Feature history for automated certificate management

Table 72: Feature History

Feature Name	Release Information	Description
Automated Certificate Management with EST and SCEP	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	With this feature, EST (Enrollment over Secure Transport) and SCEP (Simple Certificate Enrollment Protocol) helps automate the process of enrolling and renewing certificates on devices and services using Cisco SD-WAN Manager.

Automated certificate management

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

An automated certificate management on Cisco SD-WAN Manager:

- uses protocols such as EST and SCEP to automate certificate enrollment and renewal for WAN edge devices, and
- introduces enterprise certificate settings to unify certificate management across controller components, hardware WAN edges, and cloud WAN edges.

In Cisco SD-WAN Manager automatic renewal of certificates using SCEP and EST configurations occurs only during the initial device onboarding or when migrating from a hardware SUDI certificate to an enterprise certificate. For subsequent renewals, manual intervention is required to initiate the process when a certificate expiry alarm is triggered in Cisco SD-WAN Manager. Once renewal is manually initiated, the system

automatically manages the enrollment and installation of the new certificates. For more information, see Edge device certificate management .

Certificate management with Cisco SD-WAN Manager as a fabric client

Cisco SD-WAN Manager functions as a fabric client that:

- supports SCEP and EST protocols to facilitate certificate enrollment and renewal for devices,
- enables independent certificate management on Cisco SD-WAN control components and WAN edge devices, and
- enhances network security and operational flexibility.

Prerequisites for automated certificate management on CA servers

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

VPN reachability

Based on the chosen VPN (0 or 512), ensure that a route to the CA server is added, or that the CA server is reachable from the selected VPN.

Encryption algorithm

For Cisco SD-WAN Controllers, to renew certificates by configuring SCEP, the CA server should support encryption algorithm higher than triple DES.

Key size

Ensure that the minimum key size for certificates is 2048 bits or higher in CA servers.

EST configurations

- Ensure that Cisco SD-WAN Manager enrolls through the EST URL and EST is enabled on the CA. Any certificate requested from Cisco SD-WAN Manager may include custom Common Name (CN) and Organizational Unit (OU) values. The CA should be configured not to override these custom values.
- Configure a username and password for EST enrollment if configured on CA server.
- When configuring EST, you must provide the hostname or IP address that matches the digital certificate of the server. Cisco SD-WAN Manager uses hostname verification in EST client.

SCEP configurations

- Allow SCEP protocol on the CA server.
- Configure a default SCEP alias if required.
- Enable enrollment through SCEP.

- Set a higher requests-per-minute limit on the CA server to accommodate anticipated enrollment volume.
- Ensure the minimum key size for certificates is 2048 bits or higher.
- Use an encryption algorithm stronger than triple DES.

Configure certificate settings

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**

Step 2 Choose **Certificate settings** .

a) Configure the control component certificate authorization settings:

Table 73: Control Component Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise**
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.
If you choose **Enterprise** configure the following parameters.	

Field	Description
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

b) Configure the WAN edge cloud certificate authorization settings

Table 74: WAN Edge Cloud Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise** • **Automated (Manager signed)** This option is available only if you are upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.

Field	Description
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

c) Configure the hardware WAN edge certificate authorization settings

Table 75: Hardware WAN Edge Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI (SUDI certificate)** • **Enterprise**
If you choose **Enterprise** configure the following parameters.	

Field	Description
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

d) You can configure the enterprise certificate settings in advance or when you configure the certificate authorization for the control components and the WAN edge devices.

Table 76: Enterprise Certificate Settings

Field	Description
Enrollment protocol type	Choose from one of the following: • **Manual** • **EST** • **SCEP** For EST and SCEP options the route type can be vpn 0 or vpn 512, through which you can allow reachability to the CA server.
If you choose **Manual** configure the following parameters.	

Field	Description
Enterprise root certificate	Choose **Select a file** to upload a root certificate authority file. The uploaded root certificate authority displays in the text box.
If you choose **EST** configure the following parameters.	
URL base	Enter the full EST URL seen on CA server for EST/SCEP certificate authorization server.
(Optional) **Username**	Enter the username for the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Password**	Enter the password to authenticate the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **CA Label**	Enter the CA label for EST CA server. Enter the same details here as per the configurations on the CA server. Use the following format to enter the CA label: • ip-address:port and enter alias, or • host-name:port and enter alias
Root CA certificate	Click **Select a file** to upload the root CA certificate of EST/SCEP CA server. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

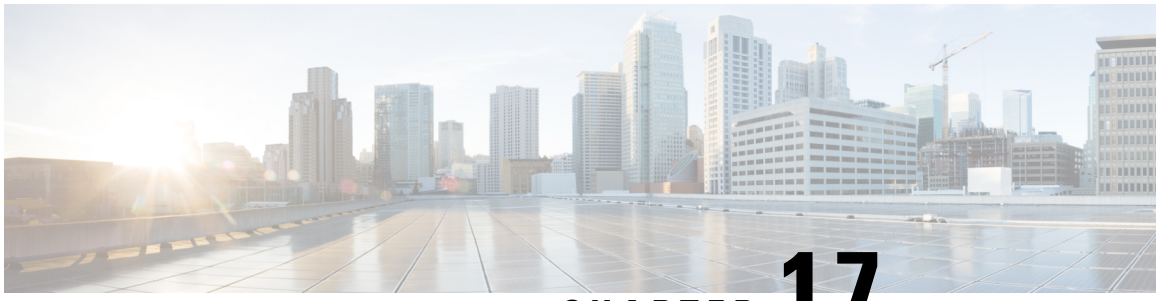
Field	Description
Generate EST Client CSR	Enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com
Upload signed certificate file	Optionally, click **Select a file** to upload a signed certificate file. The signed certificate is obtained by signing the EST client CSR manually by CA.
If you choose **SCEP** configure the following parameters.	
URL base	Enter the full SCEP URL as configured on the certificate authorization server. With this url you can call endpoints for certificate enrollment and renewal.
(Optional) **Challenge password**	Enter the password for SCEP CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Root CA fingerprint**	Use the md5 fingerprint of root CA.
Root CA certificate	Click **Select a file** to upload the root CA certificate. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

Step 3 Click **Save** .

Troubleshoot certificate management on CA server

The following table provides troubleshooting information for certificate management on CA server.

Error type	Error message	Pausible root cause	Troubleshooting steps
Internal server error	https://<est-url>:443/.well-known/est/simpleenroll HTTP Status Code: 500 500 Internal Server Error	The CA server responds with a 500 error. High CPU or memory usage on the CA server.	• Check CA server logs for error details. • Check resource utilization on CA server. • Increase resource limits if necessary.
Timeout error	Failed to get CSR signed for <device-id>, Failure reason - Read timed out HTTP Status Code: 0	The API call to the CA server times out due to resource issues in CPU, memory, or enrollment rate limits on the CA server.	Increase resource limits or enrollment rate on the CA server.
Unauthorized Error	Failed to get CSR signed for <device-id>, Failure reason - Simple Enroll: https://<est-url>:443/.well-known/est/simpleenroll HTTP Status Code: 401	• Authentication or configuration issue. • Incorrect or missing EST password. • EST client certificate lacks TLS authorization. • EST alias configurations are incorrect.	• Verify EST password in Cisco SD-WAN Manager and ensure that it matches CA server. • Check EST client certificate support for TLS authorization. • Check EST Alias configurations. • For SCEP, ensure correct challenge password is used.
EST Configuration Failure / Timeout	Loss of OMP connection with controller. Sync of root-CA certificate failed on controllers.	Failed Netconf, permission errors, or device/controller issues.	Check logs for issues on devices/controllers.



CHAPTER 17

Certificate Management

- Feature history, on page 333
- Manage Certificates in Cisco Catalyst SD-WAN Manager, on page 334
- How Cisco SD-WAN Manager installs a new certificate on an edge device, on page 345
- Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices Using Cisco SD-WAN Manager, on page 345
- Information About Configure CA Certificates Using Cisco SD-WAN Manager, on page 346
- Supported Devices for Uploading CA Certificates, on page 346
- Prerequisites to Configuring CA Certificates, on page 346
- Restrictions for Uploading CA Certificates, on page 346
- Upload CA Certificates, on page 347
- Configure CA Certificates Using Cisco SD-WAN Manager, on page 347
- Monitor CA Certificates and PKI Trustpoints, on page 349
- CRL-Based Quarantine, on page 350
- Manage Root Certificate Authority Certificates in Cisco Catalyst SD-WAN Manager, on page 352
- Enterprise Certificates, on page 353
- Cisco PKI Controller Certificates, on page 361
- Web Server Certificate for Cisco SD-WAN Manager, on page 368

Feature history

This table describes the developments of this feature, by release.

Table 77: Feature history

Feature name	Release information	Feature description
Staging for certificate installation on WAN edge devices	Cisco Catalyst SD-WAN Control Components Release 20.18.1 Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	When Cisco SD-WAN Manager installs a new certificate on a WAN edge device, the device first tests the certificate in a staging step before proceeding with installing the certificate. The device verifies that it can successfully establish control connections using the certificate.

Manage Certificates in Cisco Catalyst SD-WAN Manager

Perform certificate operations in Cisco SD-WAN Manager on the **Configuration** > **Certificates** page.

- Top bar—On the left are the menu icon, for expanding and collapsing the Cisco SD-WAN Manager menu, and the Cisco SD-WAN Manager product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Certificates.
- WAN Edge List tab—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - Send to Controllers—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - Table of WAN edge routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Controllers tab—Install certificates and download the device serial numbers to the Cisco SD-WAN Validator.



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.

  - Send to Cisco SD-WAN Validator—Send the controller serial numbers to the Cisco SD-WAN Validator.
  - Install Certificate—Install the signed certificates on the controller devices. This button is available only if you select Manual in **Administration** > **Settings** > **Certificate Signing by Symantec**.
  - Export Root Certificate—Display a copy of the root certificate for the controller devices that you can download to a file.
  - Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
  - Certificate status bar—Located at the bottom of the screen, this bar is available only if you select Server Automated in **Administration** > **Settings** > **Certificate Authorization**. It displays the states of the certificate installation process:
    - Device Added
    - Generate CSR
    - Waiting for Certificate
    - Send to Controllers

A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.

- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.

  From SD-WAN Manager 20.12.1, dates in the exported file use the Unix epoch format.
- Show Table Fields icon—Click the icon to display or hide columns from the device table. By default, all columns are displayed.

Check the WAN Edge Router Certificate Status

In the **WAN Edge List** tab, check the **Validate** column. The status can be one of the following:

- Valid (shown in green)—The router's certificate is valid.
- Staging (shown in yellow)—The router is in the staging state.
- Invalid (shown in red)—The router's certificate is not valid.

Validate a WAN Edge Router

When you add Cisco vEdge devices and WAN routers to the network using the **Configuration** > **Devices** screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox Validate the uploaded WAN Edge List and send to controllers. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the **WAN Edge List** tab, select the router to validate.
2. In the **Validate** column, click **Valid**.
3. Click **OK** to confirm the move to the valid state.
4. Repeat the steps above for each router you wish to validate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco SD-WAN Manager NMS displays the Push WAN Edge List screen showing the status of the push operation.

Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the Cisco SD-WAN Manager instance. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the Cisco SD-WAN Controller and the Cisco SD-WAN Manager instance.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the **Validate** column, click **Staging**.
3. Click **OK** to confirm the move to the staging state.
4. Click **Send to Controllers** in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. Cisco SD-WAN Manager NMS displays the **Push WAN Edge List** screen showing the status of the push operation.
5. To unstage, validate the WAN Edge Router.

Invalidate a WAN Edge Router

1. In the **WAN Edge List** tab, select the router to invalidate.
2. In the **Validate** column, click **Invalid**.
3. Click **OK** to confirm the move to the invalid state.
4. Repeat the steps above for each router you wish to invalidate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco SD-WAN Manager instance displays the **Push WAN Edge List** screen showing the status of the push operation.

Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator

To determine which controllers in the overlay network are valid, the Cisco SD-WAN Validator keeps a list of the controller serial numbers. The Cisco SD-WAN Manager instance learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the Cisco SD-WAN Validator:

1. In the **Controllers** tab, check the certificate status bar at the bottom of the screen. If the **Send to Controllers** check mark is green, all serial numbers have already been sent to the Cisco SD-WAN Validator. If it is grey, you can send one or more serial numbers to the Cisco SD-WAN Validator.



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.

2. Click the **Send to Validator** button in the **Controllers** tab. The controller's serial number and the UUIDs of the validated routers are sent to the Cisco SD-WAN Validator. If all serial numbers have been sent, when you click **Send to Validator**, an error message is displayed. To resend a controller's serial number, you must first select the device and then select **Invalid in the Validity** column.



Note In Cisco IOS XE Catalyst SD-WAN Release 17.14.x and earlier, when you click the **Send to Validator** button in the **Controllers** tab, only the controller's serial number is sent once to the Cisco SD-WAN Validator.

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.

After the serial numbers have been sent, click the **Tasks** icon in the Cisco SD-WAN Manager toolbar to display a log of the file download and other recent activities.

Install Signed Certificate

If in **Administration** > **Settings** > **Certificate Signing by Symantec**, you selected the **Manual** option for the certificate-generation process, use the **Install Certificate** button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the **Controllers** tab, click **Install Certificate**.



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.

2. In the **Install Certificate** window, select a file, or copy and paste the certificate text.
3. Click **Install** to install the certificate on the device. The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps the steps above to install additional certificates.

Export Root Certificate

1. In the **Controllers** tab, click the **Export Root Certificate** button.



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.

2. In the **Export Root Certificate** window, click **Download** to export the root certificate to a file.
3. Click **Close**.

View a Certificate Signing Request

1. In the WAN Edge List or **Controllers** tab, select a device.



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.

2. Click the **More Actions** icon to the right of the row, and click **View CSR** to view the certificate signing request (CSR).

View a Device Certificate Signing Request

1. In the **WAN Edge List** or **Controllers** tab, select a Cisco IOS XE Catalyst SD-WAN device.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

2. Click the **More Actions** icon to the right of the row, and click **View Device CSR** to view the certificate signing request (CSR).

   For a Cisco IOS XE Catalyst SD-WAN device where trustpoint has been configured, clicking the **More Actions** icon allows you to view three options:

   - View Device CSR
   - Generate Feature CSR
   - View Feature CSR



Note Cisco SD-WAN Manager will generate alarms only if device certificate is installed through Cisco SD-WAN Manager. If you install certificate manually, Cisco SD-WAN Manager will not generate alarms for certificate expiration.

View the Certificate

1. In the **Controllers** tab, select a device.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

2. Click the **More Actions** icon to the right of the row and click **View Certificate**.

Generate a Certificate Signing Request

The following procedures describe the process of generating CSRs.

Generate a controller certificate signing request, through SD-WAN Manager 20.16.x

Note From SD-WAN Manager 20.18.1, this procedure has been replaced. Use the Control Components Certificate Management workflow instead.

Procedure

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

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

3. For the desired controller, click **…** and choose **Generate CSR**.

   The **Generate CSR** window is displayed.
4. In the **Generate CSR** window, click **Download** to download the file to your local PC (that is, to the PC you are using to connect to SD-WAN Manager).
5. Repeat the preceding steps to generate a CSR for another controller.

Generate a feature certificate signing request, through SD-WAN Manager 20.16.x

Note From SD-WAN Manager 20.18.1, this procedure has been replaced. Use one of these instead:

- Control Components Certificate Management workflow
- WAN Edges Certificate Management workflow

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired device, click **…** and choose **Generate Feature CSR**.

   The **Generate Feature CSR** window is displayed.
4. In the **Generate Feature CSR** window, click **OK** to continue with the generation of feature CSR. This step authenticates the device trustpoint that has been set and extracts the CSR from the device.

5. Repeat the steps above for each device for which you are generating a CSR.

Generate a WAN edge device certificate signing request, through SD-WAN Manager 20.16.x



Note From SD-WAN Manager 20.18.x, this procedure has been replaced. Use the WAN Edges Certificate Management workflow instead.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired device, click **…** and choose **Renew Device CSR**.

   The **Renew Device CSR** window is displayed.
4. In the **Renew Device CSR** window, click **OK** to continue with the generation of a new CSR.



Note Cisco vManage Release 20.9.1 and later releases: Clicking **Renew Device CSR** resets the RSA private and public keys, and generates a CSR that uses a new key pair. SD-WAN Manager also resets RSA private and public keys before generating a new CSR in Cisco vManage Release 20.6.4 and later Cisco vManage 20.6.x releases.

SD-WAN Manager releases other than the above-mentioned releases: Clicking **Renew Device CSR** generates a CSR using the existing key pair.

Reset the RSA Key Pair

1. In the **Controllers** tab, select a device.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

2. Click the **More Actions** icon to the right of the row and click **Reset RSA**.
3. Click **OK** to confirm resetting of the device's RSA key and to generate a new CSR with new public or private keys.

Invalidate a Control Component

When invalidating the last remaining Cisco SD-WAN Validator or Cisco SD-WAN Controller in a fabric, Cisco SD-WAN Manager prompts you to set a maintenance window time in which to invalidate the component. Set a time 5 minutes or more from the current time.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **Control Components**.
2. In the **Control Components** tab, select an SD-WAN Control Component instance.

   In releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, the tab is called **Controllers**.
3. Adjacent to the SD-WAN Control Component instance, click **...** and choose **Invalidate**.

View Log of Certificate Activities

To view the status of certificate-related activities:

1. Click the **Tasks** icon located in the Cisco SD-WAN Manager toolbar. Cisco SD-WAN Manager NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco SD-WAN Manager NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

View a Signed Certificate

Signed certificates are used to authenticate Cisco SD-WAN devices in the overlay network. To view the contents of a signed certificate using Cisco SD-WAN Manager:

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



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

3. For the desired device, click **...** and choose **View Certificate** to view the installed certificate.

Certificate Revocation

Table 78: Feature History

Feature Name	Release Information	Feature Description
Certificate Revocation	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature revokes enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.

Information About Certificate Revocation

If you are using enterprise certificates with Cisco Catalyst SD-WAN, you can enable Cisco SD-WAN Manager to revoke designated certificates from devices, as needed. For example, you might need to revoke certificates if there has been a security issue at your site.

Note The certificate revocation feature is disabled by default.

Cisco SD-WAN Manager revokes the certificates that are included in a certificate revocation list (CRL) that Cisco SD-WAN Manager obtains from a root certificate authority (CA).

When you enable the Certificate Revocation feature and provide the URL of the CRL to Cisco SD-WAN Manager, Cisco SD-WAN Manager polls the root CA at a configured interval, retrieves the CRL, and pushes the CRL to Cisco IOS XE Catalyst SD-WAN devices, Cisco vEdge devices, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers in the overlay network. Certificates that are included in the CRL are revoked from devices.

When certificates are revoked, they are marked as not valid. Device control connections remain up until the next control connection flap occurs, at which time device control connections are brought down. To bring a device control connection back up, reinstall a certificate on the device and onboard the device.

When Cisco SD-WAN Manager revokes certificates from devices, the devices are not removed from the overlay network, but they are prevented from communicating with other devices in the overlay network. A peer device rejects a connection attempt from a device whose certificate is in the CRL.

Restrictions for Certificate Revocation

- By default, the Certificate Revocation feature is disabled. When you enable the Certificate Revocation feature for the first time, control connections to all the devices in the network flap. We recommend that you enable the feature for the first time during a maintenance window to avoid service disruption.

  When you disable the Certificate Revocation feature, control connections to all the devices in the network flap. We recommend that you disable the feature during a maintenance window to avoid service disruption

- You can use the Certificate Revocation feature only if you are using an enterprise CA to sign certificates for hardware WAN edge certificate authorization, controller certificate authorization, or WAN edge cloud certificate authorization.

- Cisco SD-WAN Manager can connect to a server to retrieve a CRL only through the VPN 0 interface.

Note Starting from Cisco vManage Release 20.11.1, connections through the VPN 512 are supported.

Configure Certificate Revocation

Before You Begin

Make a note of the URL of the root CA CRL.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Administration Settings** window, click **Edit** next to **Certificate Revocation List**.

   The certificate revocation options appear.
3. Click **Enabled**.
4. In the **CRL Server URL** field, enter the URL of the CRL that you created on your secure server.
5. In the **Retrieval Interval** field, enter the interval, in hours, at which Cisco SD-WAN Manager retrieves the CRL from your secure server and revokes the certificates that the CRL designates.

   Enter a value from 1 to 24. The default retrieval interval is 1 hour.
6. Click **Save**.

   Cisco SD-WAN Manager immediately retrieves the CRL and revokes the certificates that the CRL designates. From then on, Cisco SD-WAN Manager retrieves the CRL according to the retrieval interval period that you specified.

Cisco PKI Certificates

Feature Name	Release Information	Description
Support for Cisco PKI Certification	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature allows Cisco SD-WAN Manager to transition from vManage signed certificates to Cisco PKI as the default certificate method for virtual routers to enhance security and reliability.

Cisco PKI Certificates

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

Cisco SD-WAN public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

PKI provides a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or a device) participating in the secured communicated is enrolled in the PKI in a process where the entity generates an Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has their identity validated by a trusted entity also known as a CA or trustpoint.

Before Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager signed certificates were installed on the controller devices by default. From Cisco Catalyst SD-WAN Manager Release 20.18.1, Virtual routers use a Cisco PKI certificate by default. After you reset a WAN edge device, you have to install the certificates manually on the device. If you perform an upgrade, your certificate is retained.

Note When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1 or later, the Cisco SD-WAN Controllers continues to support Cisco SD-WAN Manager signed certificate if it is already enabled. However, when the certificates are renewed, the Cisco SD-WAN Controllers have a PKI certificate by default.

Renew a Certificate

Before You Begin

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Certificate settings**. Click any one of the following options and choose enterprise mode to enable the CRL (certificate revocation list).
  - In the **Certificate Signing by** field, choose **Cisco (Recommended)** or **Manual** or **Enterprise Certificate** .
  - When you choose **Cisco (Recommended)**, click **Sync Root Certificate** to sync root certificate to all the connected devices.
  - In the **Validity Period** field, choose the duration.
  - Click **Save**.

Note By default, the **Cisco (Recommended)** option is disabled.

To renew Certificates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired controller, click **…** and choose **Renew CSR**.

   The **Renew CSR** window is displayed.

The certificates are renewed in the following order:

1. Cisco SD-WAN Manager
2. Cisco SD-WAN Validator
3. Cisco SD-WAN Controller
4. Cisco IOS XE Catalyst SD-WAN device

Note When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1 or later, the Cisco SD-WAN Controllers continues to support vManage signed certificate if it is already enabled. However, when the certificates are the renewed, the Cisco SD-WAN Controllers have PKI certificate by default.

How Cisco SD-WAN Manager installs a new certificate on an edge device

In a Cisco Catalyst SD-WAN environment, edge devices use certificates for authorization when establishing control connections with SD-WAN Control Components. From SD-WAN Manager 20.18.1, when SD-WAN Manager installs a new certificate on a device, the device first tests the certificate in a staging step before proceeding with installing the certificate. During the staging step, the device verifies that it can successfully establish a control connection to the SD-WAN Validator, using the certificate. If the SD-WAN Validator cannot validate the certificate, it rejects the connection.

Workflow

1. SD-WAN Manager stages a certificate on a WAN edge device.
2. The device attempts to connect to the SD-WAN Validator, using the staged certificate for authorization. Staging and testing can take a minute or more.
   - If the certificate is valid and if the SD-WAN Validator recognizes the certificate, it accepts the control connection.
   - If the certificate is invalid or if the SD-WAN Validator does not recognize the certificate, it rejects the control connection.
3. The edge device reports the staging result back to SD-WAN Manager: success or failure.
   - In case of success, SD-WAN Manager completes the installation of the certificate on the device.
   - In case of failure, SD-WAN Manager does not proceed to install the certificate, and adds a log entry indicating the failure.

Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices Using Cisco SD-WAN Manager

Table 79: Feature History

Feature Name	Release Information	Description
Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Using Cisco SD-WAN Manager, conveniently upload and push generic third-party CA certificates to Cisco IOS XE Catalyst SD-WAN devices with a Trustpoint name. The provisioning is executed via configuration groups parcel, with the status readily viewable in monitoring.

Information About Configure CA Certificates Using Cisco SD-WAN Manager

The Cisco SD-WAN Manager currently permits the upload of third party certificates to devices during their integration with the Cisco Catalyst SD-WAN fabric, yet this function is only available during the control connection establishment and initial device setup.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the feature enables certificate upload using the UI. The Cisco SD-WAN Manager supports CA certificate uploads even after device setup.

The CA certificates authenticate the server identities and prevent unauthorized access. The Cisco IOS XE Catalyst SD-WAN devices use CA certificates to establish and manage secure connections with different servers in a network. When you upload a CA certificate to Cisco SD-WAN Manager, the Cisco IOS XE Catalyst SD-WAN device uses this certificate information from the configuration group parcels in verifying and authenticating the connections it establishes with servers across a network, thus improving the overall security and integrity of your network traffic.



Note The CA certificates isn't suited for SSL-based access with router trusted roots.

Supported Devices for Uploading CA Certificates

Cisco IOS XE Catalyst SD-WAN devices

Prerequisites to Configuring CA Certificates

- Your Cisco SD-WAN Manager must run Cisco Catalyst SD-WAN Manager Release 20.13.1 and later releases to upload CA certificates.
- Your Cisco IOS XE Catalyst SD-WAN device must run Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and later releases to upload CA certificates.

Restrictions for Uploading CA Certificates

- Supports only PEM encoded certificate files.
- Maximum certificate file size: 10 MB.
- If you are using Cisco Catalyst SD-WAN Multitenancy, you need to be a tenant to upload and manage CA certificates. For more information see, Tenant Role.

Note When you login into Cisco SD-WAN Manager as a provider, you can't upload and manage CA certificates.

Upload CA Certificates

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click the **CA Cert** tab.
3. Click **Add CA Certificate**.
4. In the **Add CA Certificate** pane, enter **Certificate Name**.
5. **Choose a file** or drag and drop to upload a CA certificate.
6. Click the **Paste** tab and paste the certificate details.
7. Click **Save**.

   On the **Certificate Authority** page, find the CA certificate listed in the **Device Group** table.

Note Spot the **Expiration Date** in the **Device Group** table for your CA certificate and perform more **Actions** by clicking the **. . .** icon.

Delete CA Certificates

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click the **CA Cert** tab.
3. In the **Device Group** table, select the CA certificate to delete.
4. Click **Delete**.

Note Alternate method to delete a CA certificate: click the **...** icon in the **Actions** column and click **Delete**.

Configure CA Certificates Using Cisco SD-WAN Manager

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

   For more information on creating a configuration group, see Configuration Group Workflows.
2. Add a feature to the configuration group.

For more information on adding a feature, see Feature Management.

3. Under **System Profile**, click **Add Feature**.
4. In the **Add Feature** pane, choose **CA Certificate**.
5. Configure the **CA Certificates** section.

Table 80: CA Certificates

Field	Description
Type	Choose **CA Certificate** from the drop-down list.
Name	Enter a name for the certificate.
Description	(Optional) Provide a description for the certificate.
Add CA Certificate	Click **Add CA Certificate** to add additional CA certificates.
TrustPoint Name	Enter a TrustPoint Name.
Certificate Name	Choose a CA certificate to add from the drop-down list.

6. Click **Save**.
7. Deploy the devices associated to the configuration group. For more information, see Deploy Devices.

Note When you modify a certificate from the **Device Group** table, the changes won't be mirrored on the device. This is due to the certificate's association with a TrustPoint. To update the certificate, it's necessary to remove the existing TrustPoint that contains the certificate information. Subsequently, create a new TrustPoint and add the certificate to it. Finally, deploy the changes to the device for the certificates to take effect.

Deleting certificates from the **Certificates** tab doesn't automatically delete the associated TrustPoint. To delete the TrustPoint, you must manually delete and then save the changes to the TrustPoint.

Revoke the CA Certificates

Use the following instructions to revoke a CA certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **...** adjacent to the configuration group name and choose **Edit**.
3. Click the desired system profile.
4. Click **...** adjacent to the CA certificate feature and choose **Delete Feature**.
5. Deploy the changes to the device.

Renew the CA Certificates

Use the following instructions to renew a CA certificate:

1. Upload the CA certificate that you'd like to renew to the Cisco SD-WAN Manager.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
3. Click **...** adjacent to the configuration group name and choose **Edit**.
4. Click the desired system profile.
5. Click **...** adjacent to the CA certificate feature and choose **Delete Feature**.
6. Using **Configuration Groups**, add a feature to the configuration group and follow the instructions from step 3 to step 7 in the **Configure CA Certificate topic**.

Monitor CA Certificates and PKI Trustpoints

Track CA Certificate

Track a CA certificate using the **Issuer Name**, **Certificate Serial No.**, and **Expiration Date** listed in the Cisco SD-WAN Manager.

1. In the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click the **CA Cert** tab.
3. The CA certificate added to Cisco SD-WAN Manager appears in the **Device Group** table.

Monitor CA Certificate Installation

Once the CA certificate installation is complete, the Cisco IOS XE Catalyst SD-WAN device sends the event logs to Cisco Catalyst SD-WAN Manager.

From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.

The CA certificate installation is listed as an event and appears in the **Events** table.

Monitor PKI Trustpoints

Monitor PKI Trustpoints using the real time command **`PKI Trustpoint`**. For more information, see View PKI Trustpoint information.

CRL-Based Quarantine

Table 81: Feature History

Feature Name	Release Information	Feature Description
CRL-Based Quarantine	Cisco vManage Release 20.11.1	With this feature you can quarantine SD-WAN edge devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a certificate authority.

Information About CRL-Based Quarantine

When you use enterprise certificates with Cisco Catalyst SD-WAN, you can use Cisco SD-WAN Manager to quarantine SD-WAN edge devices that are compromised, and their certificates have been revoked.

Note The certificate revocation list (CRL)-based quarantine feature is disabled by default.

- Cisco SD-WAN Manager revokes the certificates that are included in a certificate revocation list (CRL). Cisco SD-WAN Manager obtains this list from a certificate authority (CA).
- At defined intervals, Cisco SD-WAN Manager polls the CRL server for the latest CRL. On receiving the list, Cisco SD-WAN Manager analyzes it to determine which SD-WAN edge device is to be quarantined.
- Cisco SD-WAN Manager checks if the serial numbers of certificates for each valid SD-WAN edge device in the network match the serial numbers of certificates within the CRL. On finding a match, the certificates on the SD-WAN edge devices are not removed to enable the SD-WAN edge devices to retain a control connection to Cisco SD-WAN Manager.

The quarantine process for SD-WAN edge devices is as follows:

- For each SD-WAN edge device that is quarantined:
  - Cisco SD-WAN Manager moves the SD-WAN edge device to the staging mode. The staging mode shuts down data traffic while maintaining a control connection to Cisco SD-WAN Manager.
  - Cisco SD-WAN Manager generates notifications for the SD-WAN edge device being quarantined.

For each Cisco SD-WAN Controller that is quarantined, Cisco SD-WAN Manager generates notifications for the controller.

Note The CRL server connects to Cisco SD-WAN Manager through VPN 0 or VPN 512.

Restrictions for CRL-Based Quarantine

- You can use the CRL-based quarantine feature only if you have an enterprise CA (certificate authority) to sign certificates for hardware WAN edge certificate authorization, controller certificate authorization, or WAN edge cloud certificate authorization.
- Disable the CRL to switch from certificate revocation to quarantine or quarantine to certificate revocation. You cannot enable the certificate revocation and CRL-based quarantine option at the same time.

Configure CRL-Based Quarantine

Before You Begin

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**. Click any one of the following options and choose enterprise mode to enable the CRL (certificate revocation list).
  - In the **Controller Certificate Authorization** field, choose **Enterprise Root Certificate** or
  - In the **Hardware WAN Edge Certificate Authorization** field, choose **Enterprise Certificate (signed by Enterprise CA)** or
  - In the **WAN Edge Cloud Certificate Authorization** field, choose **Manual (Enterprise CA - recommended)**.
- Make a note of the URL of the CA CRL.



Note By default, the CRL-based quarantine feature is disabled.

To configure CRL-based quarantine:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Administration Settings** page, click **Edit** next to **Certificate Revocation List**.

   The Certificate Revocation and CRL-Based Quarantine options appear.
3. Click **CRL-Based Quarantine**.
4. In the **CRL Server URL** field, enter the URL of the CRL that you created on your secure server.
5. In the **Retrieval Interval** field, enter the interval in hours. Cisco SD-WAN Manager uses the certificate revocation list (CRL) to quarantine SD-WAN edge devices.

   Enter a value from 1 to 24. The default retrieval interval is 24 hours.
6. Click **VPN 0** or **VPN 512**. Cisco SD-WAN Manager connects to a server to retrieve the CRL through the VPN 0 or VPN 512 interface.
7. Click **Save**.

   Cisco SD-WAN Manager at intervals, polls the CRL server for the latest CRL. This list is analyzed to determine which SD-WAN edge devices are to be quarantined.

Note If the CRL is disabled in earlier releases, the CRL remains disabled after upgrading to the Cisco vManage Release 20.11.1. If the CRL was enabled in a release prior to Cisco vManage Release 20.11.1, then after upgrading to Cisco vManage Release 20.11.1, the certificate revocation option is enabled with VPN0 as the default.

Manage Root Certificate Authority Certificates in Cisco Catalyst SD-WAN Manager

Feature Name	Release Information	Description
Support for Managing Root CA Certificates in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature enables you to add and manage root certificate authority (CA) certificates.

Add a Root Certificate Authority Certificate

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. In the **Root Certificate** field, paste in certificate text, or click **Select a File** to load a certificate from a file.
4. Click **Add**. The new certificate appears in the certificate table. The **Recent Status** column indicates that the certificate has not yet been installed.
5. Click **Next** and review the details of any certificates that have not been installed.
6. Click **Save** to install the certificate(s). The new certificate appears in the certificate table.

View a Root Certificate Authority Certificate

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. (optional) In the search field, enter text to filter the certificate view. You can filter by certificate text or attribute values, such as serial number.
3. In the table of certificates, click **More Actions** (**…**) and choose **View**. A pop-up window appears, displaying the certificate and its details.

Delete a Root Certificate

Before you begin

Note When you make changes to the root certificate chain, SD-WAN Manager automatically propagates the changes to SD-WAN Validator and SD-WAN Controller instances.

Use this procedure to delete a root Certificate Authority (CA) certificate.

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. Select one or more root certificates in the table and click the **trash** icon in the **Action** column. The table shows the certificate as marked for deletion.
4. Click **Next** and review the details of any certificates that are marked for deletion.
5. Click **Save** to delete the certificate(s).

Enterprise Certificates

Feature Name	Release Information	Description
RSA Key Length Increase in Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Control Components Release 20.15.2 Cisco Catalyst SD-WAN Control Components Release 20.16.1	Introduces 4096-bit RSA key support for certificate signing requests (CSR) for enterprise certificates.

In Cisco IOS XE SD-WAN Release 16.11.1 and Cisco SD-WAN Release 19.1, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization used previously. For purposes of certificate management, the term *controller* is used to collectively refer to Cisco SD-WAN Manager, the Cisco Catalyst SD-WAN Controller, and the Cisco Catalyst SD-WAN Validator.

RSA Key Length

When using enterprise certificates for Cisco SD-WAN Controllers, ensure that you use root certificates with an RSA key that is at least 2048 bits.

From Cisco Catalyst SD-WAN Control Components Release 20.16.1 and Cisco Catalyst SD-WAN Control Components Release 20.15.2, Cisco SD-WAN Control Components support RSA key sizes ranging from 2048 to 4096 bits.

Downgrade Restriction

If you are using enterprise certificates that use 4096-bit RSA keys, before downgrading Cisco SD-WAN Control Components to a release earlier than Cisco Catalyst SD-WAN Control Components Release 20.16.1Cisco Catalyst SD-WAN Control Components Release 20.15.2, change the enterprise certificates to use 2048-bit RSA keys.

Note For more information about enterprise certificates, see the Cisco Catalyst SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide.

Use the Certificates page to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco Catalyst SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from Cisco SD-WAN Manager that you generate these certificates and install them on the controller devices—Cisco SD-WAN Manager, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers.
- The WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco Catalyst SD-WAN, mark each router as valid or invalid, and then from Cisco SD-WAN Manager, send the file to the controller devices in the network.

Install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

Configure Enterprise Certificates for Cisco SD-WAN Controllers

Feature Name	Release Information	Description
Support for Secondary Organizational Unit	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco SD-WAN Release 20.1.1	This optional feature allows you to configure a secondary organizational unit when configuring the certificates. If specified, this setting is applied to all controllers and edge devices.
Support for Subject Alternative Name (SAN)	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature enables you to configure subject alternative name (SAN) DNS Names or uniform resource identifiers (URIs). It enables multiple host names and URIs to use the same SSL certificate.

Feature Name	Release Information	Description
Support for Specifying Any Organization for WAN Edge Cloud Device Enterprise Certificates	Cisco Catalyst SD-WAN Control Components Release 20.11.1	When configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization in the **Organization** field. You are not limited to names such as **Viptela LLC**, **vIPtela Inc**, or **Cisco Systems**. This enables you to use your organization's certificate authority name or a third-party certificate authority name.
Support for Certificates Without the Organizational Unit Field	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Control Components Release 20.12.1	Enterprise certificates that you install on devices do not require the Organizational Unit (OU) field to be defined. Earlier, this field was used as part of the authentication of a device.

Information About Enterprise Certificates

Enterprise certificates allow organizations to use their own private certificate signing authority rather than having to rely on public certificate signing authorities. You can also apply custom certificate properties using the **Set CSR Properties** field.



Note In the 16.11/19.1 release, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization that were used previously. An independent organization handles the signing of enterprise certificates.

Use the **Configuration** > **Certificates** page to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco Catalyst SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from Cisco SD-WAN Manager that you generate these certificates and install them on the controller devices—Cisco SD-WAN Manager instances, Cisco SD-WAN Validators, and Cisco SD-WAN Controller.
- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco Plug and Play (PnP), mark each router as valid or invalid, and then from Cisco SD-WAN Manager, send the file to the controller devices in the network.

You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

Note For purposes of certificate management, the term controller refers collectively to Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.

Once you reset a WAN edge device, you have to install the enterprise root certificate manually on the device. If you perform an upgrade, your certificate is retained.

Note Cisco SD-WAN Manager supports only Base 64 encoded certificates. Other formats, such as DER, encoded are not supported.

For example, the PEM extension is used for different types of X.509v3 files that contain ASCII (Base64) armored data prefixed with a **--BEGIN ...** line.

Dependency on OU Fields in Enterprise Certificates

From Cisco Catalyst SD-WAN Control Components Release 20.12.1, when onboarding a device, Cisco Catalyst SD-WAN does not require that the associated enterprise certificate have any OU fields defined. However, if at least one OU field is defined, then Cisco Catalyst SD-WAN requires that one of the OU fields match the organization name of the fabric.

From Cisco Catalyst SD-WAN Control Components Release 20.12.2, when onboarding a device, if the associated enterprise certificate has one or more OU fields defined, the OU fields need not match the organization name of the fabric.

Devices that Support Enterprise Certificates

Device	Enterprise Certificate Support
Cisco SD-WAN Manager	Yes
Cisco SD-WAN Validator	Yes
Cisco SD-WAN Controller	Yes
Edge routers	All hardware WAN edge routers vEdge/IOS-XE-SD-WAN except ASR1002-X, ISRv, CSR1000v

Configure Enterprise Certificates

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Hardware WAN Edge Certificate Authorization**.
2. Click **Enterprise Certificate** (signed by Enterprise CA).

   On Box Certificate (TPM/SUDI Certificate) is the default option.

3. If you want to specify custom certificate properties, click **Set CSR Properties** and configure the following properties.

Property	Description
Domain Name	Network domain name. Do not exceed 17 characters.
Organizational Unit	This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. **Note** For devices using Cisco IOS XE Catalyst SD-WAN Release 17.9.3a or later releases of Cisco IOS XE Release 17.9.x, or Cisco IOS XE Catalyst SD-WAN Release 17.12.1a or later, the certificates that you install on the devices do not require the Organizational Unit field to be defined. However, if a signed certificate includes the Organizational Unit field, the field must match the organization name configured on the device. This addresses the policy of the Certification Authority Browser Forum (CA/Browser Forum), as of September 2022, to stop including an organizational unit in signed certificates. Despite the change in policy of the CA/Browser Forum, some certificate authorities might still include an organizational unit in the signed certificate.
Secondary Organization Unit	This optional field is available from Cisco IOS XE Release 17.2 or Cisco SD-WAN Release 20.1.x. If this optional field is specified, it will be applied to all controllers and edge devices. **Note** If a signed certificate includes the Organizational Unit field or the Secondary Organizational Unit field, one of these fields must match the organization name configured on the device. This addresses the policy of the Certification Authority Browser Forum (CA/Browser Forum), as of September 2022, to stop including an organizational unit in signed certificates. Despite the change in policy of the CA/Browser Forum, some certificate authorities might still include an organizational unit in the signed certificate.
Organization	Organization name.
City	City name.
State	State name.
Email	Email address.
2-Letter Country Code	Country code.
Subject Alternative Name (SAN) DNS Names	Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com

Property	Description
Subject Alternative Name (SAN) URIs	Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

4. Choose **Select a file** to upload a root certificate authority file.

   The uploaded root certificate authority displays in the text box.

5. Click **Save**.

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

7. Select the **Upload WAN Edge List** tab.

8. Browse to the location of the Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices list and click **Upload**.

9. On the **Configuration** > **Certificates** page, click **...** and choose an action:

   - **View Enterprise CSR** (certificate signing request): Copy the CSR and sign it using the enterprise root certificate, and upload the signed certificate on Cisco SD-WAN Manager using the Install Certificate operation. Cisco SD-WAN Manager automatically discovers on which hardware edge the certificate needs to be installed on.
   - **View Enterprise Certificate**: After the certificate is installed, you can see the installed certificate and download it.
   - **Renew Enterprise CSR**: If you need to install a new certificate on the hardware device, you can use the Renew Enterprise CSR option. The Renew Enterprise CSR option generates the CSR. You can then view the certificate (View Enterprise CSR option) and install the certificate (Install Certificate option). This step flaps the control connections as a new serial number. You can see the new serial number and expiry data on the Configuration > Certificates page.

Note The certificates that you install on devices in the Cisco Catalyst SD-WAN overlay do not require the Organizational Unit field to be defined. However, if a signed certificate includes the Organizational Unit field, the field must match the organization name configured on the device.

   - **Revoke Enterprise Certificate**: This option removes the enterprise certificate from the device and moves it back to prestaging. The device has only Cisco SD-WAN Validator and Cisco SD-WAN Manager controls up.

   For a Cisco IOS XE Catalyst SD-WAN device, click **...** and choose an action:

   - **View Feature CSR**:
     - Copy the CSR available from the Cisco IOS XE Catalyst SD-WAN device.
     - Sign the certificate using the enterprise root certificate from a certifying authority.
     - Upload the signed certificate on Cisco SD-WAN Manager using the **Install Feature Certificate** operation.

Cisco SD-WAN Manager automatically discovers on which hardware edge the certificate needs to be installed. After you install feature certificate, the option **View Feature Certificate** is available.

- **View Feature Certificate**: After you install the feature certificate, you can view the feature certificate and download it.
- **Revoke Feature Certificate**: This option removes the feature certificate or trustpoint information from the Cisco IOS XE Catalyst SD-WAN device. After revoking a certificate, all actions against devices are not available. To view all actions for a device, ensure that you configure logging information of the device to a Transport Layer Security (TLS) profile with authentication type as server, and then configure back to mutual. Alternatively, to view the actions, reset Cisco IOS XE Catalyst SD-WAN device to factory default configuration.

  To reset a device to factory default:

  - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
  - Create a device template with the factory-default template.

    The factory-default template is, Factory_Default_*feature-name*_Template. See Create a Device Template from Feature Templates for information about creating a device template with feature template.

10. Click **Install Certificate** or **Install Feature Certificate** to upload the signed certificate.

    The certificate must be a signed certificate. Initially, the state is CSR Generated.

    The state changes to Certificate Installed when successfully installed.
11. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**. You can see enterprise certificate columns, including the device type, chassis-id, enterprise serial number, and enterprise certificate date.

Invalidate a Device Certificate

Before deleting a WAN edge device, invalidate the device.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. In the row showing the device, click **Invalid** to invalidate the device.

Authorize a Controller Certificate for an Enterprise Root Certificate

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Controller Certificate Authorization** area, click **Edit**.
3. Click **Enterprise Root Certificate**. If a warning appears, click **Proceed** to continue.
4. Optionally, click **Set CSR Properties** to configure certificate signing request (CSR) details manually.

Note In a multi-tenant scenario, if you configure CSR properties manually and if you are using Cisco Catalyst SD-WAN Control Components Release 20.11.1 or later, then ensure that devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.11.1a or later. In a single-tenant scenario, this is not required.

In a multi-tenant scenario, if you configure CSR properties manually, then when you are ready to generate a CSR for a tenant device, enter the tenant's organization name in the **Secondary Organizational Unit** field described below. In a multi-tenant scenario, if you are generating a CSR for a service provider device, this is not required.

The following properties appear:

- **Domain Name**: Network domain name. Maximum 17 characters.
- **Organizational Unit**

Note **Organizational Unit** is a noneditable field. This field is auto-filled with the organization name that you have configured for Cisco SD-WAN Manager in **Administration** > **Settings** > **Organization Name**.

- **Secondary Organizational Unit**: This optional field is only available in Cisco IOS XE Release 17.2 or Cisco SD-WAN Release 20.1.x and onwards. Note that if this optional field is specified, it will be applied to all controllers and edge devices.
- **Organization**: Beginning with Cisco vManage Release 20.11.1, when configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization in this field. You are not limited to names such as **Viptela LLC**, **vIPtela Inc**, or **Cisco Systems**. This enables you to use your organization’s certificate authority name or a third-party certificate authority name. The maximum length is 64 characters, and can include spaces and special characters. Cisco SD-WAN Manager validates the name when you enter it.
- **City**
- **State**
- **Email**
- **2-Letter Country Code**
- **Subject Alternative Name (SAN) DNS Names**: (optional) You can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com
- **Subject Alternative Name (SAN) URIs**: (optional) You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

5. Paste an SSL certificate into the **Certificate** field or click **Select a file** and navigate to an SSL certificate file.
6. (Optional) In the **Subject Alternative Name (SAN) DNS Names** field, you can enter multiple host names to use the same SSL certificate.

   Example: cisco.com and cisco2.com

7. (Optional) In the **Subject Alternative Name (SAN) URIs** field, you can enter multiple URIs to use the same SSL certificate.

   Example: cisco.com and support.cisco.com

   This is helpful for an organization that uses a single certificate for a host name, without using different subdomains for different parts of the organization.

Generate a Bootstrap Configuration

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive or from internal boot flash to a device that supports SD-WAN. When the device boots, it uses the information in the configuration file to come up on the network.

Note If you need to generate a bootstrap configuration, use the **Configuration** > **Devices** page, click **…**, and choose **Generate Bootstrap Configuration**.

Note Beginning with Cisco vManage Release 20.7.1, there is an option available when generating a bootstrap configuration file for a Cisco vEdge device, enabling you generate two different forms of the bootstrap configuration file.

- If you are generating a bootstrap configuration file for a Cisco vEdge device that is using Cisco Catalyst SD-WAN Release 20.4.x or earlier, then check the **The version of this device is 20.4.x or earlier** check box.
- If you are generating a bootstrap configuration for a Cisco vEdge device that is using Cisco SD-WAN Release 20.5.1 or later, then do not use the check box.

Cisco PKI Controller Certificates

From software release 19.x and onwards, there is an option to use Cisco as the certificate authority (CA) instead of Symantec/Digicert for Cisco Catalyst SD-WAN controller certificates.

This section describes deployment types, scenarios to administer, install, and troubleshoot controller certificates using Cisco public key infrastructure (PKI). Cisco PKI provides certificate management to support security protocols such IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

The major difference between Symantec/Digicert and Cisco PKI certificates is that Cisco PKI certificates are linked to a Smart Account (SA) and Virtual Account (VA) in Plug and Play (PnP) and do not require manual approval using a portal like Digicert. Each VA has a limit of 100 certificates, meaning that each overlay has a limit of 100 certificates, and after the certificate signing request (CSR) is generated, the approval and installation happens automatically if the Cisco SD-WAN Manager settings are set correctly.

Devices are added and certificates are installed automatically from the Cisco PKI servers. No intervention is required to approve the certificate.

Supported Devices for Cisco PKI Certificates

The following are the supported devices for using Cisco PKI certificates.

Device	Support
Cisco SD-WAN Manager	Yes
Cisco Catalyst SD-WAN Validator	Yes
Cisco Catalyst SD-WAN Controller	Yes
Cisco vEdge devices	Yes
Cisco IOS XE Catalyst SD-WAN devices	Yes

Use Cases for Cisco PKI Controller Certificates

- Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above, on page 362
- Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal, on page 364
- Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers, on page 367

Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above

Prerequisites

Cisco SD-WAN Manager and the controllers should all be running the same software version.

On the **Configuration** > **Devices** > **Controllers** page, ensure that the OOB IP address and credentials are updated for all the controllers.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

You can verify the software version for the new or expired overlays without having control connections using SSH.

1. SSH to each of the controllers and the version should show during the SSH process.
2. You do not need to actually have the credentials work, therefore you can run this on a controller where the credentials do not work.

   Repeat this process for all the controllers in the overlay to make sure.
3. Customer Smart Account credentials need to be ready using either of the following methods:
   a. Email and request the customer contact from PnP trigger notifications to individually email you and provide the Smart Account credentials.

      or

b. Email and request the customer contact to log on to Cisco SD-WAN Manager and add them. Also ensure that you ask the customer for their IPs to be added to the allowed list..

Ensure that if asking the customer to provide their customer contact to log on, this step is done after asking the customer for their IPs to be added to the allowed list, so that they can reach the Cisco SD-WAN Manager GUI, be be able to log in, and input their Smart Account credentials.

To find your Smart Account credentials, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials** .

Enter the user name and password and click **Save**.

Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Controller Certificate Authorization** and click **Edit**.
3. Click **Cisco (Recommended)**.



Note Cisco SD-WAN Manager displays an error if the Smart Account credentials are not added. Check the prerequisites.

4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press Save.



Note Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the Cisco SD-WAN Manager GUI.

   From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers**. Click **…** and choose **Generate CSR**.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   The operation status shows the CSR sent for signing, the certificate signed and installed automatically without needing human intervention.

7. The certificates are installed automatically. If successful, the **Configuration** > **Certificates** > **Controllers** page shows the following:

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

- Expiration date for the certificates for each controller
- Operation Status column:
  - Cisco SD-WAN Validator: "Installed"
  - Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller: "Cisco SD-WAN Validator Updated"
- Certificate Serial column: Certificate serial number

8. Ensure that the control connections have come up to the controllers on the Cisco SD-WAN Manager dashboard.

Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal

Prerequisites

Cisco SD-WAN Manager, controllers, and vEdges should all have their control connections up.

Ensure OOB IP address and credentials are updated in **Configuration** > **Devices** > **Controllers**.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

For each controller, click **…** and verify the updates.

Migrate an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates

1. In Cisco SD-WAN Manager, verify that the control connections to controllers and Cisco vEdge devices are up.

   If the control connections are not up, migrating from Digicert to Cisco PKI cannot proceed.

   If the control connections are only partially up, that is some Cisco vEdge devices are control down, then those Cisco vEdge devices will not be able to automatically reconnect to the controllers if their control comes up after the certificates have been moved to Cisco PKI.

   If it is a case of expired certificates and control connections are down, then certificates need to be renewed on Digicert first and control connections need to be brought up before migrating them to the Cisco PKI controller certificates.

2. Verify that the software version of the controllers is 19.x or later.

How to Verify the Software Version for the Active Existing Overlays (with Valid Control Connections to Controllers) Using Cisco SD-WAN Manager

a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.

b. Click **Manager** and check the **Current Version** column. Verify that it is 19.x or later.

If the control connections are up and Cisco SD-WAN Manager and controller versions are not 19.x or later, then upgrade them first (Cisco vEdge devices need not be upgraded) before migration to Cisco PKI can be done.



Note It is mandatory that controllers upgraded to 19.x should immediately have their certificates renewed with Cisco PKI as part of the upgrade; they cannot be allowed to run with the existing Symantec certificates even if those certificates are going to remain valid.

c. After verifying the prerequisites, check that the Cisco PKI root-CA has been propagated to all the controllers and the Cisco vEdge devices. This requires SSH access to the controllers.

1. SSH into the Cisco SD-WAN Manager and controllers and run the following command: **show certificate root-ca-cert | include Cisco**.

   If the output is blank or does not show the result, escalate to the cloud infrastructure team.

d. Customer Smart Account credentials need to be ready by either of the following methods:

1. Email and request the customer contact from a PnP trigger notification to individually email you and provide the Smart Account credentials.

   or

2. Email and request your customer contact to log on to the Cisco SD-WAN Manager themselves and add them. Also ensure that you ask for the customer IPs to be added to the allowed list.

   Ensure that if asking the customer to provide, this step is done after asking the customer for their IPs to be added to the allowed list, so that they can reach the Cisco SD-WAN Manager GUI, be able to log on, and input the Smart Account Credentials.

   To view the Smart Account credentials, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and see the **Smart Account Credentials** section.

3. Enter the username and password and click **Save**.

   Once all the prerequisites have been satisfied, follow the **Runbook to Request and Install Cisco PKI Certificates** procedure to request CSRs and get the Cisco certificates installed. Verify that all the control connections to the controllers and the Cisco vEdge devices have come back up. If not, then escalate to the cloud infrastructure team.

Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**, and in the **Controller Certificate Authorization** section, click **Edit**.

3. Click **Cisco (Recommended)**.



Note Cisco SD-WAN Manager displays an error if the Smart Account credentials are not added. Check the prerequisites.

4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press Save.



Note Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the Cisco SD-WAN Manager GUI.

   From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers** . Click **…** and choose **Generate CSR**.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   The operation status shows the CSR sent for signing, the certificate signed and installed automatically without requiring intervention.

7. The certificates are installed automatically. If successful, the **Configuration** > **Certificates** > **Controllers** page shows the following:



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   - Expiration date for the certificates for each controller
   - Operation Status column:
     - Cisco SD-WAN Validator: "Installed"
     - Cisco SD-WAN Manager and Cisco SD-WAN Controller: "Cisco SD-WAN Validator Updated"
   - Certificate Serial column: Certificate serial number

8. Ensure that the control connections have come up to the controllers on the Cisco SD-WAN Manager dashboard.
9. Set the Certificate Retrieve Interval to 1 minute.

10. Click **Sync Root Certificate** to migrate the Cisco vEdge devices or Cisco IOS XE Catalyst SD-WAN devices in Cisco SD-WAN Manager to Cisco pki. This support available from 19.2.1 version or later.
11. Click **Save**.

Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers

The following steps require access to PnP and to the SA/VA in question. Customers have access to their own SA/VA.

Prerequisites

The prerequisites are the same in the above cases, except that you use the manual method for installing the certificates.

Runbook

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**. In the **Controller Certificate Authorization** section, verify that it is set to Manual.
2. Generate the CSRs for the controllers.

   From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers**.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   Click **…** and choose **Generate CSR**.

   Download each CSR to a file with a filename `.csr` and keep it ready to submit to the PnP portal for getting the signed certificates.
3. Log on to the PnP portal to the required SA/VA and select the Certificates tab.
4. Click **Generate Certificate** and follow the steps to give a name for the certificate file, paste the CSR, and download the signed certificate.

   The finished certificate is ready for download. Repeat this process for each CSR and download all the required certificates.
5. To install the downloaded certificates, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers**.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The **Controllers** tab is renamed as **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   Click **Install Certificate**.

   After installation, verify that the control connections are up.

Debugging and Log Information

1. Check the Cisco Catalyst SD-WAN Validator profile under the VA in PnP to verify that the correct organization name exists.
2. Check the output at `/var/log/nms/vmanage-server.log` on Cisco SD-WAN Manager for logs of the entire certificate process.
3. Verify that Cisco SD-WAN Manager has internet connectivity to reach the Cisco PKI servers.

Web Server Certificate for Cisco SD-WAN Manager

To establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you must generate a CSR to create a certificate, have it signed by a root CA, and then install it. You must install a separate certificate on each Cisco SD-WAN Manager server in a cluster by performing the following steps for each server:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Web Server Certificate** area, click **CSR**.
3. In the **Common Name** field, enter the domain name or IP address of the Cisco SD-WAN Manager server. For example, the fully-qualified domain name of Cisco SD-WAN Manager could be vmanage.org.local.
4. In the **Organizational Unit** field, enter the unit name within your organization — for example, Network Engineering.
5. In the **Organization** field, enter the exact name of your organization as specified by your root CA — for example, Viptela Inc.
6. In the **City** field, enter the name of the city where your organization is located — for example, San Jose.
7. In the **State** field, enter the state in which your city is located — for example, California.
8. In the **2-Letter Country Code** field, enter the two-letter code for the country in which your state is located. For example, the two-letter country code for the United States of America is US.
9. Click **Validity** and choose the validity period for the certificate.
10. Optionally, in the **Subject Alternative Name (SAN) DNS Names** field, enter the names of DNS severs to which the certificate trust should be extended. If you enter more than one DNS server name, separate each name with a space or a comma.



Note Cisco Catalyst SD-WAN supports SAN DNS names, from Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

11. Optionally, in the **Subject Alternative Name (SAN) URIs** field, enter the URIs of resources to which the certificate trust should be extended. If you enter more than one URI, separate each URI with a space or a comma.

Enter each URI in *scheme*:*value* format, where *scheme* is the protocol for accessing the resource and *value* is the resource. For example, **`https://example.example.com`** or **`scp://example.example.com`**.



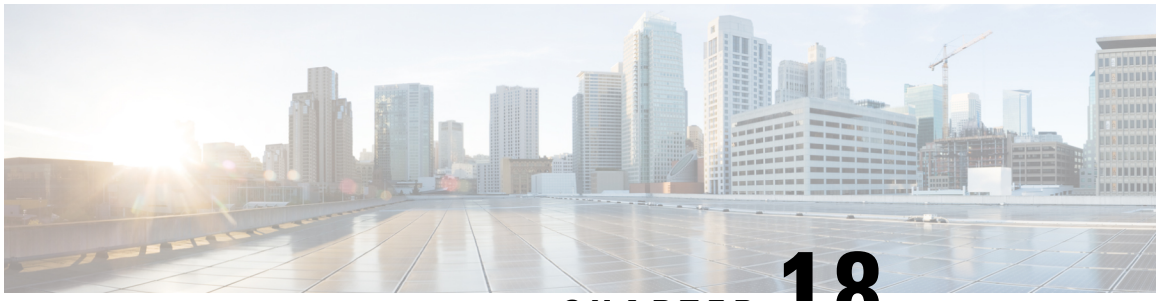
Note Cisco Catalyst SD-WAN supports SAN URIs beginning with Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

12. Click **Generate** to generate the CSR.
13. Send the CSR to your CA server to have it signed.
14. When you receive the signed certificate, click **Certificate** near the **Web Server Certificate** bar to install the new certificate. The **View** box displays the current certificate on the Cisco SD-WAN Manager server.
15. Copy and paste the new certificate in the box. Alternatively, click **Import** and **Select a File** to download the new certificate file.
16. Restart the application server and log in to Cisco SD-WAN Manager.

View Web Server Certificate Expiration Date

When you establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, configure the time period for which the certification is valid (in Step 8 in the previous section). At the end of this time period, the certificate expires. The **Web Server Certificate** bar shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco SD-WAN Manager dashboard displays a notification indicating that the certificate will expire soon. This notification is then displayed again 30, 15, and 7 days before the expiration date, and then daily.



CHAPTER 18

Cisco SD-WAN Control Components Certificate Management

- SD-WAN Control Components certificate management feature history, on page 371
- Control Components Certificate Management workflow, on page 371
- Supported environments for the Control Components Certificate Management workflow, on page 372
- Supported components for the Control Components Certificate Management workflow, on page 372
- Renew Certificates using the Control Components Certificate Management workflow, on page 372

SD-WAN Control Components certificate management feature history

Table 82: Feature History

Feature Name	Release Information	Description
SD-WAN Control Components Certificate Management workflow	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Control Components Release 20.18.1	The Control Components Certificate Management workflow updates the authentication certificates for SD-WAN Control Components in the fabric. This is useful for updating certificates before they expire.

Control Components Certificate Management workflow

The Control Components Certificate Management Workflow in Cisco SD-WAN Manager is a step-by-step interactive procedure (called a workflow) that updates the authentication certificates for SD-WAN Control Components.

Cisco Catalyst SD-WAN uses authentication certificates to authenticate components when establishing control connections between SD-WAN Control Components, or between SD-WAN Control Components and edge devices. SD-WAN Manager can manage the certificates installed on components in the network:

- SD-WAN Control Components
- WAN edge devices

Certificates expire and require renewal. Use this SD-WAN Manager workflow to renew the certificates for SD-WAN Control Components.

Expired certificates

From SD-WAN Control Components 20.18.1, control connections between SD-WAN Control Components and edge devices remain operational even when the certificates on SD-WAN Control Components have expired. Control connections may also successfully re-establish after being manually cleared, including connections to SD-WAN Controllers with expired certificates. This maintains the functionality of the fabric.

Supported environments for the Control Components Certificate Management workflow

The workflow applies to Cisco Catalyst SD-WAN environments in which you manage the SD-WAN Control Components.

Supported components for the Control Components Certificate Management workflow

- Cisco SD-WAN Manager
- Cisco SD-WAN Controller
- Cisco SD-WAN Validator

Renew Certificates using the Control Components Certificate Management workflow

The Control Components Certificate Management workflow provides two methods:

- **Auto**: For each selected SD-WAN Control Component, SD-WAN Manager generates a certificate signing request (CSR), sends the CSR to the certificate authority (CA) for signing, then installs the signed certificate on the component.

  The **Auto** option is available if you have selected one of the Cisco PKI, EST, or SCEP options in **Administration** > **Settings** > **Certificate settings**.

- **Manual**: For each selected SD-WAN Control Component, SD-WAN Manager generates a certificate signing request (CSR) for you to download. Then you manually handle the certificate signing and re-upload the signed certificate. The workflow then installs the signed certificate on the component.

Before you begin

For the automatic certificate signing option that occurs in the workflow, two prerequisites apply. Without these, only a manual signing option is available in the workflow. Here are the prerequisites:

- Smart Account and Virtual Account

  In Cisco Catalyst SD-WAN Manager Release 20.18.1 and earlier, enter Smart Account and Virtual Account details in Cisco SD-WAN Manager.

  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials**.
  2. Enter your Smart Account or Virtual Account credentials in the **Username** and **Password** fields.

- Register Plug-and-Play

  From Cisco Catalyst SD-WAN Manager Release 20.18.2, service providers in a multitenant environment and tenant in a single-tenant environment must register the Plug-and-Play service.

- Certificate signing by Cisco

  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Certificate settings**.
  2. Click **Control Components**.
  3. Change **Certificate Signing by** to **Cisco**.

Procedure

Step 1 Do one of these to launch the Control Components Certificate Management workflow:

- Launch from the workflow library.
  a. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
  b. Launch the Control Components Certificate Management workflow.

- Launch from the **Control Components** page.
  a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components**.
  b. Click **Certificate management** to launch the Control Components Certificate Management workflow.

Step 2 Choose **Auto** or **Manual**, select the desired SD-WAN Control Components, and proceed according to the instructions in the workflow.

For the **Manual** option:

- File formats

  If you use the **Manual** option, which requires you to complete the signing for each certificate manually, outside of SD-WAN Manager, add the signed certificates to a single archive file to upload at the required step. The workflow supports these file formats for upload:

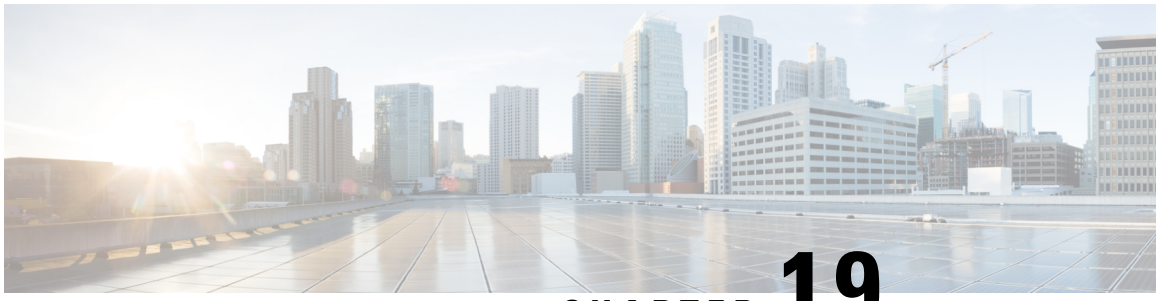
  - zip

- pem
- crt
- cer

If you are renewing certificates for multiple SD-WAN Control Components simultaneously, we recommend using the zip format so that you can combine all certificates into a single zip file to upload.

- Signed certificates

  If you use the **Manual** option, which requires you to complete the signing for each certificate manually, the archive file that you upload with the signed certificates must include a signed certificate for each selected SD-WAN Control Component. If the uploaded file does not contain signed certificates for each, the workflow does not proceed.



CHAPTER 19

Edge device certificate management

- Edge device certificate management feature history, on page 375
- Edge device certificate management, on page 376
- Edge device certificate management feature history, on page 376
- WAN edge device certificate management workflow, on page 376
- Supported components for the edge device certificate management workflow, on page 376
- Supported solutions for the edge device certificate management workflow, on page 376
- Renew certificates using the edge device certificate management workflow, on page 377

Edge device certificate management feature history

Table 83: Feature History

Feature Name	Release Information	Description
WAN edge device certificate management workflow	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Control Components Release 20.18.1	The WAN edge device certificate management workflow updates the authentication certificates for edge devices in the fabric. This is useful for updating certificates before they expire.

Edge device certificate management

Edge device certificate management feature history

Table 84: Feature History

Feature Name	Release Information	Description
WAN edge device certificate management workflow	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Control Components Release 20.18.1	The WAN edge device certificate management workflow updates the authentication certificates for edge devices in the fabric. This is useful for updating certificates before they expire.

WAN edge device certificate management workflow

The WAN Edges Certificate Management Workflow in Cisco SD-WAN Manager is a step-by-step interactive procedure (called a workflow) that updates the authentication certificates for edge devices in the network.

SD-WAN Manager uses authentication certificates on WAN edge devices to communicate with other network components in the fabric.

Certificates expire and require renewal. Use this SD-WAN Manager workflow to renew the certificates for edge devices.

Supported components for the edge device certificate management workflow

- Cisco IOS XE Catalyst SD-WAN devices
- Cisco vEdge devices

Supported solutions for the edge device certificate management workflow

The workflow applies to WAN edge devices in the SD-WAN or SD-Routing solutions.

Renew certificates using the edge device certificate management workflow

The WAN Edges Certificate Management workflow provides two methods:

- Auto: For each selected WAN edge device, SD-WAN Manager generates a certificate signing request (CSR), sends the CSR to the certificate authority (CA) for signing, then installs the signed certificate on the device.
- Manual: For each selected WAN edge device, SD-WAN Manager generates a certificate signing request (CSR) for you to download. Then you manually handle the certificate signing and re-upload the signed certificate. The workflow then installs the signed certificate on the device.

Before you begin

For the automatic certificate signing option in the workflow, two prerequisites apply. If these are not met, only a manual signing option is available in the workflow. The prerequisites are:

- Smart Account and Virtual Account

  In Cisco Catalyst SD-WAN Manager Release 20.18.1 and earlier, enter Smart Account and Virtual Account details in Cisco SD-WAN Manager.

  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials**.
  2. Enter your Smart Account or Virtual Account credentials in the **Username** and **Password** fields.

- Register Plug-and-Play

  From Cisco Catalyst SD-WAN Manager Release 20.18.2, service providers in a multitenant environment and tenant in a single-tenant environment must register the Plug-and-Play service.

- Certificate signing by Cisco

  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Certificate settings**.
  2. Click **WAN Edges for 20.18.x and above**.
  3. Change **Certificate Signing by** to **Cisco**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Launch the WAN Edges Certificate Management workflow.

Step 3 Choose **Auto** or **Manual**, select the desired WAN edge devices, and proceed according to the instructions in the workflow.

The workflow lists each WAN edge device, and the certificate information for each, including expiration date.

- File formats

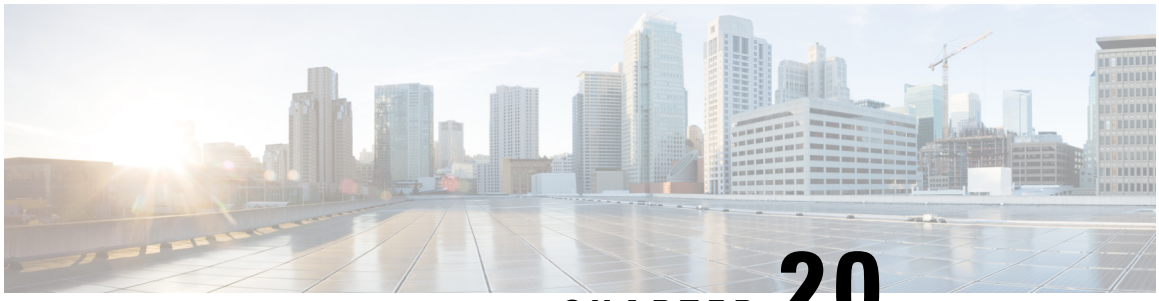
If you use the **Manual** option, which requires you to complete the signing for each certificate manually, outside of SD-WAN Manager, add the signed certificates to a single archive file to upload at the required step. The workflow supports these file formats for upload:

- zip
- pem
- crt
- cer

If you are renewing certificates for multiple devices simultaneously, we recommend using the zip format so that you can combine all certificates into a single zip file to upload.

- Signed certificates

  If you use the **Manual** option, which requires you to complete the signing for each certificate manually, the archive file that you upload with the signed certificates must include a signed certificate for each selected device. If the uploaded file does not contain signed certificates for each, the workflow does not proceed.



CHAPTER 20

Expired Enterprise Certificate Indication and Quarantine

- Expired Certificate Indication and Quarantine, on page 379
- Information About Expired Certificate Indication and Quarantine, on page 379
- Enable Quarantining Devices with Expired Certificates, on page 381
- View and Remedy Devices in Expired Certificate Quarantine, on page 381

Expired Certificate Indication and Quarantine

Table 85: Feature History

Feature Name	Release Information	Feature Description
Expired Certificate Indication and Quarantine	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Control Components Release 20.16.1	Cisco SD-WAN Manager indicates when devices or Cisco Catalyst SD-WAN Control Components have expired certificates. Additionally, you can quarantine all edge devices that have expired certificates. Quarantine places devices into the staging status. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.

Information About Expired Certificate Indication and Quarantine

Indication of Expired Certificates

A digital certificate is used to authenticate devices in the overlay network. After authentication, devices and Cisco Catalyst SD-WAN Control Components can establish secure sessions with one another. A certificate is issued by a certificate authority and has an expiration date.

Every several minutes, Cisco SD-WAN Manager checks the devices and Cisco Catalyst SD-WAN Control Components in the network for expired certificates. If it detects any expired certificates, Cisco SD-WAN Manager displays a banner with a link to the **Configuration** > **Certificates** > **WAN Edges** page or **Configuration** > **Certificates** > **Control Components** page to show the details of which devices or components require certificate renewal.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the Cisco SD-WAN Manager UI parses certificate expiration dates by using the **expirationdatelong** command (epoch time), ensuring consistency across all time zones.

Device Quarantine

Quarantine refers to placing devices into a staging state. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.

You can quarantine devices that have expired certificates. See Enable Quarantining Devices with Expired Certificates, on page 381.

Quarantining devices with expired certificates enforces the requirement to renew an expired certificate. Removing network elements with expired certificates may be necessary to comply with an organization's network security requirements.

This table shows which devices are subject to automatic quarantine when the quarantine feature is enabled.

Table 86: Automatic Quarantine for Expired Certificate

Device or Control Component	Automatic Quarantine, When Quarantine Enabled?
Hardware devices using a certificate	Yes
Hardware devices using an on-box trusted platform module (TPM) secure unique device identifier (SUDI) certificate	No
Software devices	Yes
Cisco Catalyst SD-WAN Control Components	No

Multitenancy

In a multitenancy scenario, enabling quarantine for expired certificates is possible only at the provider level and applies to all tenants.

Enable Quarantining Devices with Expired Certificates

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Device Quarantine**.

Step 3 Enable device quarantine.

View and Remedy Devices in Expired Certificate Quarantine

Cisco SD-WAN Manager can quarantine devices with expired certificates. See Information About Expired Certificate Indication and Quarantine, on page 379. It does not quarantine Cisco SD-WAN Control Components.

Before you begin

Enable quarantine for expired certificates. See Enable Quarantining Devices with Expired Certificates, on page 381.

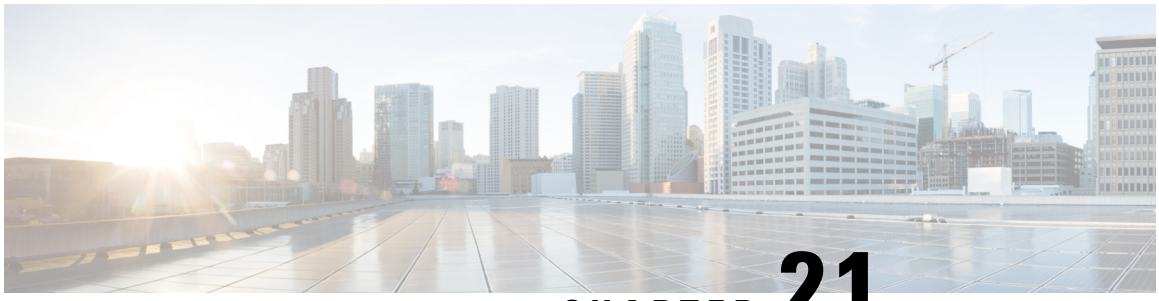
Procedure

Step 1 Open the **Configuration** > **Certificates** > **WAN Edges** page to show a table with details of which devices require certificate renewal.

If Cisco SD-WAN Manager is displaying a banner message indicating that one or more devices are quarantined for expired certificates, click the link in the banner message to open the page.

In the table, an exclamation point icon indicates a problem with a device. Hover over the icon to display the details of the problem, such as an expired certificate. If a device is quarantined, the **Validate** column for the device shows **staging**.

Step 2 To remove a device from quarantine, renew its certificate. See Generate a WAN Edge Device Certificate Signing Request.



CHAPTER 21

Reverse Proxy

- Reverse Proxy, on page 383
- Information About Reverse Proxy, on page 383
- Restrictions for Reverse Proxy, on page 385
- Provision Certificates on the Reverse Proxy, on page 386
- Configure Reverse Proxy Using Cisco SD-WAN Manager, on page 387
- Monitor Reverse Proxy Using CLI, on page 389
- Monitor Reverse Proxy Using CLI, on page 393

Reverse Proxy

Table 87: Feature History

Feature Name	Release Information	Description
Support for Reverse Proxy with Cisco Catalyst SD-WAN and Cisco Catalyst SD-WAN Multitenancy	Cisco IOS XE Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	With this feature, you can deploy a reverse proxy in your overlay network between Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager and Cisco SD-WAN Controllers. Also, this feature enables you to deploy a reverse proxy in both single-tenant and multitenant deployments that include Cisco vEdge devices or Cisco IOS XE Catalyst SD-WAN devices. In a multitenant deployment, the service provider manages reverse proxy and the associated configuration.

Information About Reverse Proxy

In a standard overlay network, Cisco Catalyst SD-WAN edge devices initiate direct connections to the Cisco SD-WAN Control Components (Cisco SD-WAN Manager and Cisco SD-WAN Controller s) and exchange control plane information over these connections. The WAN edge devices are typically located in branch sites and connect to the Cisco SD-WAN Controller s over the internet. As a result, Cisco SD-WAN Manager and Cisco SD-WAN Controller s are also connected directly to the internet.

For security, or other reasons, you may not want the Cisco SD-WAN Controller s to have direct internet connections. In such a scenario, you can deploy a reverse proxy between the Cisco SD-WAN Controller s and the WAN edge devices. The reverse proxy acts as an intermediary to pass control traffic between the Cisco SD-WAN Controller s and the WAN edge devices. Instead of communicating directly with Cisco SD-WAN Manager and the Cisco SD-WAN Controller s, the WAN edge devices communicate with the reverse proxy, and the reverse proxy relays the traffic to and from Cisco SD-WAN Manager and Cisco SD-WAN Controller s.

The following figure illustrates a reverse proxy deployed between a WAN edge device and Cisco SD-WAN Manager and the Cisco SD-WAN Controller s.

You can deploy a reverse proxy in both single-tenant and multi-tenant Cisco Catalyst SD-WAN deployments. The TLOC communicates with the reverse proxy on its public IP address and port, regardless of public or private TLOC.

Support for a Device with Both Private Network and Public Internet Connectivity

You can use a reverse proxy in a Cisco Catalyst SD-WAN network that includes a device with these multiple TLOCs:

- A TLOC that connects to an internal private network without internet access, and
- A TLOC that connects to the public internet

This scenario has a specific requirement for configuring the TLOC color of each Cisco SD-WAN Controller. This table describes this special case. For comparison, the table includes examples of devices with only one TLOC, and devices that have separate TLOCs for a private network and the public internet.

Table 88: TLOC Color Requirements

Device	TLOC	TLOC Connectivity	Configure this TLOC Color as a...	The Device Connects to this Cisco SD-WAN Validator	Connectivity to: Cisco SD-WAN Controller, and Cisco SD-WAN Manager	Specific TLOC Color Requirements
A	1	Internal private network	Private color Example: private1	Cisco SD-WAN Validator reachable through the private network	Direct connectivity through the private network	None

Device	TLOC	TLOC Connectivity	Configure this TLOC Color as a...	The Device Connects to this Cisco SD-WAN Validator	Connectivity to: Cisco SD-WAN Controller, and Cisco SD-WAN Manager	Specific TLOC Color Requirements
B	1	Public internet	Public color Example: custom1	Cisco SD-WAN Validator reachable through the public internet	Connectivity through a reverse proxy	None
C	1	Internal private network	Private color Example: private1	Cisco SD-WAN Validator reachable through the private network	Direct connectivity through the private network	A network that includes a device with multiple TLOCs as shown here has this specific requirement: Configure the TLOCs for each Cisco SD-WAN Controller with the private color that you are using for the private network. Do not leave the TLOC color as default. Leaving the TLOC color for the Cisco SD-WAN Controllers as the default color causes this problem: Devices with a TLOC connecting to the internal private nework, such as Device C, cannot connect to the Cisco SD-WAN Controllers.
	2	Public internet	Public color Example: custom1	Cisco SD-WAN Validator reachable through the public internet	Connectivity through a reverse proxy	

Restrictions for Reverse Proxy

- Multitenant scenario

  In a multitenant Cisco Catalyst SD-WAN overlay network, you can deploy a reverse proxy device with only a three-node Cisco SD-WAN Manager cluster.

- TLS-based control plane

  Deployment of the reverse proxy is only supported with a TLS-based control plane for Cisco SD-WAN Manager and Cisco SD-WAN Controllers.

- Cisco vEdge 5000 router restriction

  You cannot deploy a reverse proxy with a Cisco vEdge 5000 router.

- IPv6

  You cannot deploy a reverse proxy with IPv6 control connections.

- Devices with a TLOC for a private WAN

  The following restriction applies to edge devices in a scenario in which (a) one or more devices have a TLOC connecting them to a private WAN, and (b) one or more Cisco SD-WAN Validators do not have reachability to a reverse proxy:

  In this scenario, Zero-Touch Provisioning (ZTP) onboarding does not support onboarding a Cisco IOS XE Catalyst SD-WAN device with a TLOC using the default TLOC color. Bootstrap the device with a minimal configuration that configures a non-default TLOC color.

Provision Certificates on the Reverse Proxy

Before exchanging traffic, the reverse proxy and the WAN edge devices must authenticate each other.

On the reverse proxy you must provision a certificate that is signed by the CA that has signed the certificate of the Cisco SD-WAN Controllers. This certificate is used by the reverse proxy to verify the WAN edge devices.

From Cisco IOS XE Catalyst SD-WAN Release 17.15.x, initial connection establishment for WAN edge devices in reverse proxy topologies may take a few additional minutes to complete.

To generate a Certificate Signing Request (CSR) for the reverse proxy and have it signed by Cisco, do as follows:

1. Run the following command on the reverse proxy:

   ```
   proxy$ openssl req -new -days 365 -newkey rsa:2048 -nodes -keyout Proxy.key -out Proxy.csr
   ```

   When prompted, enter values as suggested in the following table:

Property	Description
Country Name (2 letter code)	Any country code. Example: US
State or Province Name	Any state or province. Example: CA
Locality Name	Any locality. Example: San Jose

Property	Description
Organization Name	Use either "vIPtela Inc" or "Viptela LLC". Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, you can use "Cisco Systems" string as the Organization Name for enterprise certificates. Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1 you cannot include a comma in the **Organization Name** field of the bootstrap configuration file. Example: Viptela LLC
Organizational Unit Name	Use the “organization” name configured on the overlay. Example: cisco-sdwan-12345
Common Name	Host name ending with “.viptela.com”. Example: proxy.viptela.com
Email Address	Use any valid email address. Example: someone@example.com

2. Get the CSR signed by Cisco.
   - If you use Symantec/Digicert as the CA for the Cisco SD-WAN Controllers, open a case with Cisco TAC to sign the CSR.
   - If you use Cisco Public Key Infrastructure (PKI) as the CA for the Cisco SD-WAN Controllers, submit the CSR on the Cisco Network Plug and Play (PnP) application and retrieve the signed certificate.

Configure Reverse Proxy Using Cisco SD-WAN Manager

Configure Reverse Proxy Settings

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **Reverse Proxy** setting, click **Edit**.
3. For **Enable Reverse Proxy**, click **Enabled**.
4. Click **Save**.

Configure Reverse Proxy Settings on Cisco SD-WAN Controllers

1. From the Cisco SD-WAN Manager menu, choose **Configure** > **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.

3. For the desired Cisco SD-WAN Manager instance or Cisco SD-WAN Controller, click **…** and click **Add Reverse Proxy**.

   The **Add Reverse Proxy** dialog box appears.

4. To map a private IP address and port number to a proxy IP address and port number, do as follows:

   a. Click **Add Reverse Proxy**.

   b. Enter the following details:

Private IP	The private IP address is the IP address of the transport interface in VPN 0.
Private Port	This is the port used to establish the connections that handle control and traffic in the overlay network. The default port number is 12346.
Proxy IP	Proxy IP address to which private IP address must be mapped.
Proxy Port	Proxy port to which the private port must be mapped.

   c. If the Cisco SD-WAN Manager instance or Cisco SD-WAN Controller has multiple cores, repeat **Step 4 a** and **Step 4 b** for each core.

5. To delete a private IP address-port number to proxy IP address-port number mapping, find the mapping and click the trash icon.

6. To save the reverse proxy settings, click **Add**.

   To discard the settings, click **Cancel**.

7. In the Security feature template attached to the Cisco SD-WAN Manager instance or Cisco SD-WAN Controller, choose TLS as the transport protocol.

After you configure reverse proxy settings on a Cisco SD-WAN Manager instance or a Cisco SD-WAN Controller, WAN edge devices in the overlay network are provisioned with a certificate for authentication with the reverse proxy.

1. When a reverse proxy is deployed, Cisco SD-WAN Validator shares the details of the reverse proxy with the WAN edge devices.

2. On learning about the reverse proxy, a WAN edge device initiates the installation of a signed certificate from Cisco SD-WAN Manager.

3. After the certificate is installed, the WAN edge device uses the certificate for authentication with the reverse proxy and connects to the reverse proxy.

Disable Reverse Proxy

Note Before you disable reverse proxy, delete any private IP address-port number to proxy IP address-port number mappings that you have configured for Cisco SD-WAN Manager instances and Cisco SD-WAN Controller. See *Configure Reverse Proxy Settings on Cisco Catalyst SD-WAN Controllers* for information about deleting the mappings.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **Reverse Proxy** setting, click **Edit**.
3. For **Enable Reverse Proxy**, click **Disabled**.
4. Click **Save**.

Monitor Reverse Proxy Using CLI

Monitor Private and Proxy IP Address and Port Numbers of WAN Edge Devices on Cisco SD-WAN Controllers

The following is a sample output from the execution of the **show control connections** command on a Cisco SD-WAN Controller. In the command output, for a WAN edge device, the entries in the PEER PRIVATE IP and PEER PRIV PORT columns are the configured TLOC IP address and port number of the WAN edge interface. The entries in the PEER PUBLIC IP and PEER PUB PORT columns are the corresponding IP address and port number of the reverse proxy interface. The same command can also be executed on a Cisco SD-WAN Manager instance to obtain a similar output.

```
vsmart1# show control connections
                                                                    PEER                 PEER
      PEER    PEER PEER            SITE       DOMAIN PEER         PRIV    PEER         PUB
INDEX TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP   PORT    PUBLIC IP    PORT
    ORGANIZATION   REMOTE COLOR     STATE UPTIME
------------------------------------------------------------------------------------------------
0     vbond   dtls 172.16.1.2         0          0      10.1.1.2     12346   10.1.1.2
12346   EXAMPLE-ORG    default         up     53:08:18:50
0     vmanage tls  172.16.1.6         1          0      10.2.100.6   45689   10.2.100.6
45689   EXAMPLE-ORG    default         up     53:08:18:32
1     vedge   tls  1.1.100.1       100        1      10.3.1.2     57853   10.2.100.1  53624
   EXAMPLE-ORG    biz-internet    up     53:08:18:44
1     vedge   tls  1.1.101.1       101        1      10.4.1.2     55411   10.2.100.1  53622
   EXAMPLE-ORG    biz-internet    up     53:08:18:48
1     vbond   dtls 172.16.1.2         0          0      10.1.1.2     12346   10.1.1.2
12346   EXAMPLE-ORG    default         up     53:08:18:51

vsmart1#
```

View Mapping of SD-WAN Controller Private IP Address and Port Number to Proxy IP Address and Port Number on Cisco SD-WAN Validator

The following is a sample output from the execution of the **show orchestrator reverse-proxy-mapping** command on a Cisco SD-WAN Validator. In the command output, the entries in the PROXY IP and PROXY

PORT columns are the proxy IP address and port number. The entries in the PRIVATE IP and PRIVATE PORT columns are the private IP address and port number of the transport interface in VPN 0.

```
vbond# show orchestrator reverse-proxy-mapping

                                                    PRIVATE             PROXY
UUID                                   PRIVATE IP   PORT     PROXY IP   PORT
------------------------------------------------------------------------------
14c35ae4-69e3-41c5-a62f-725c839d25df   10.2.100.4   23456    10.2.1.10  23458
14c35ae4-69e3-41c5-a62f-725c839d25df   10.2.100.4   23556    10.2.1.10  23558
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   23456    10.2.1.10  23457
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   23556    10.2.1.10  23557
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   23656    10.2.1.10  23657
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   23756    10.2.1.10  23757
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   23856    10.2.1.10  23857
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   23956    10.2.1.10  23957
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   24056    10.2.1.10  24057
6c63e80a-8175-47de-a455-53a127ee70bd   10.2.100.6   24156    10.2.1.10  24157

vbond#
```

Example: View Mapping of SD-WAN Controller Private IP Address and Port Number to Proxy IP Address and Port Number on a WAN Edge Device

The following is a sample output from the execution of the **show sdwan control connections** command on a Cisco IOS XE Catalyst SD-WAN device. In the command output, check the entry in the PROXY column for a Cisco SD-WAN Manager instance or a Cisco SD-WAN Controller. If the entry is Yes, the entries in the PEER PUBLIC IP and PEER PUBLIC PORT are the proxy IP address and port number.

```
Device# show sdwan control connections

                                                                    PEER              PEER
                           CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER              PRIV  PEER        PUB
                           GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP        PORT  PUBLIC IP   PORT
ORGANIZATION    LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------------------------------------------

vsmart  tls  172.16.1.4         1          1      10.2.100.4    23558 10.2.1.10   23558
EXAMPLE-ORG     biz-internet    Yes   up     52:08:44:25 0

vbond   dtls 0.0.0.0          0          0      10.1.1.2      12346 10.1.1.2    12346
EXAMPLE-ORG     biz-internet    -     up     52:08:50:47 0
```

```
vmanage tls  172.16.1.6         1          0      10.2.100.6    23957 10.2.1.10   23957
EXAMPLE-ORG     biz-internet    Yes   up     66:03:04:50 0



Device#
```

On a Cisco vEdge device, you can obtain a similar output by executing the command **show control connections**.

View Signed Certificate Installed on a WAN Edge Device for Authentication with Reverse Proxy

The following is a sample output from the execution of the **show sdwan certificate reverse-proxy** command on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# show sdwan certificate reverse-proxy

Reverse proxy certificate

------------------


Certificate:

    Data:

        Version: 1 (0x0)

        Serial Number: 1 (0x1)

        Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

        Validity

            Not Before: Jun  2 19:31:08 2021 GMT

            Not After : May 27 19:31:08 2051 GMT

        Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78, O
 = ViptelaClient
        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                RSA Public-Key: (2048 bit)

                Modulus:

                    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:

                    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:

                    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:

                    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:

                    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:

                    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:
```

```
                    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:

                    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:

                    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:

                    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:

                    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:

                    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:

                    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:

                    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:

                    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:

                    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:

                    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:

                    34:9b

                Exponent: 65537 (0x10001)

    Signature Algorithm: sha256WithRSAEncryption

         99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:

         b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:

         07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
         33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:

         c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:

         af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:

         7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:

         61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:

         0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:

         d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:

         3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:

         88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:

         19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:

         06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:

         2f:31:02:59


Device#
```

On a Cisco vEdge device, you can obtain a similar output by executing the command **show certificate reverse-proxy**.

Monitor Reverse Proxy Using CLI

Monitor Private and Proxy IP Address and Port Numbers of WAN Edge Devices on Cisco SD-WAN Controllers

The following is a sample output from the execution of the **show control connections** command on a Cisco SD-WAN Controller. In the command output, for a WAN edge device, the entries in the PEER PRIVATE IP and PEER PRIV PORT columns are the configured TLOC IP address and port number of the WAN edge interface. The entries in the PEER PUBLIC IP and PEER PUB PORT columns are the corresponding IP address and port number of the reverse proxy interface. The same command can also be executed on a Cisco SD-WAN Manager instance to obtain a similar output.

```
vsmart1# show control connections
                                                                    PEER                 PEER
      PEER    PEER PEER            SITE       DOMAIN PEER         PRIV    PEER         PUB
INDEX TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP   PORT    PUBLIC IP    PORT
    ORGANIZATION   REMOTE COLOR     STATE UPTIME
------------------------------------------------------------------------------------------------
0     vbond   dtls 172.16.1.2         0          0      10.1.1.2     12346   10.1.1.2
12346   EXAMPLE-ORG    default         up     53:08:18:50
0     vmanage tls  172.16.1.6         1          0      10.2.100.6   45689   10.2.100.6
45689   EXAMPLE-ORG    default         up     53:08:18:32
1     vedge   tls  1.1.100.1       100        1      10.3.1.2     57853   10.2.100.1  53624
   EXAMPLE-ORG    biz-internet    up     53:08:18:44
1     vedge   tls  1.1.101.1       101        1      10.4.1.2     55411   10.2.100.1  53622
   EXAMPLE-ORG    biz-internet    up     53:08:18:48
1     vbond   dtls 172.16.1.2         0          0      10.1.1.2     12346   10.1.1.2
12346   EXAMPLE-ORG    default         up     53:08:18:51

vsmart1#
```

View Mapping of SD-WAN Controller Private IP Address and Port Number to Proxy IP Address and Port Number on Cisco SD-WAN Validator

The following is a sample output from the execution of the **show orchestrator reverse-proxy-mapping** command on a Cisco SD-WAN Validator. In the command output, the entries in the PROXY IP and PROXY PORT columns are the proxy IP address and port number. The entries in the PRIVATE IP and PRIVATE PORT columns are the private IP address and port number of the transport interface in VPN 0.

```
vbond# show orchestrator reverse-proxy-mapping

                                                PRIVATE             PROXY
UUID                                    PRIVATE IP  PORT     PROXY IP   PORT
------------------------------------------------------------------------------
14c35ae4-69e3-41c5-a62f-725c839d25df  10.2.100.4  23456    10.2.1.10  23458
14c35ae4-69e3-41c5-a62f-725c839d25df  10.2.100.4  23556    10.2.1.10  23558
6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  23456    10.2.1.10  23457
6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  23556    10.2.1.10  23557
```

```
6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  23656    10.2.1.10  23657

6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  23756    10.2.1.10  23757

6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  23856    10.2.1.10  23857

6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  23956    10.2.1.10  23957

6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  24056    10.2.1.10  24057

6c63e80a-8175-47de-a455-53a127ee70bd  10.2.100.6  24156    10.2.1.10  24157


vbond#
```

Example: View Mapping of SD-WAN Controller Private IP Address and Port Number to Proxy IP Address and Port Number on a WAN Edge Device

The following is a sample output from the execution of the **show sdwan control connections** command on a Cisco IOS XE Catalyst SD-WAN device. In the command output, check the entry in the PROXY column for a Cisco SD-WAN Manager instance or a Cisco SD-WAN Controller. If the entry is Yes, the entries in the PEER PUBLIC IP and PEER PUBLIC PORT are the proxy IP address and port number.

```
Device# show sdwan control connections

                                                                    PEER              PEER
                           CONTROLLER

PEER    PEER PEER            SITE       DOMAIN PEER          PRIV  PEER        PUB
                           GROUP

TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP    PORT  PUBLIC IP   PORT
ORGANIZATION    LOCAL COLOR     PROXY STATE UPTIME      ID
--------------------------------------------------------------------------------------------------------------------

vsmart  tls  172.16.1.4         1          1      10.2.100.4    23558 10.2.1.10   23558
EXAMPLE-ORG     biz-internet    Yes   up     52:08:44:25 0

vbond   dtls 0.0.0.0         0          0      10.1.1.2      12346 10.1.1.2    12346
EXAMPLE-ORG     biz-internet    -     up     52:08:50:47 0

vmanage tls  172.16.1.6         1          0      10.2.100.6    23957 10.2.1.10   23957
EXAMPLE-ORG     biz-internet    Yes   up     66:03:04:50 0


Device#
```

On a Cisco vEdge device, you can obtain a similar output by executing the command **show control connections**.

View Signed Certificate Installed on a WAN Edge Device for Authentication with Reverse Proxy

The following is a sample output from the execution of the **show sdwan certificate reverse-proxy** command on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# show sdwan certificate reverse-proxy

Reverse proxy certificate
```

```
------------------


Certificate:

    Data:

        Version: 1 (0x0)

        Serial Number: 1 (0x1)

        Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

        Validity

            Not Before: Jun  2 19:31:08 2021 GMT

            Not After : May 27 19:31:08 2051 GMT

        Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78, O
 = ViptelaClient
        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                RSA Public-Key: (2048 bit)

                Modulus:

                    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:

                    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:

                    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:

                    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:

                    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:

                    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:

                    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:

                    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:

                    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:

                    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:

                    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:

                    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:

                    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:

                    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:

                    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:

                    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:
```

```
                    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:

                    34:9b

                Exponent: 65537 (0x10001)

    Signature Algorithm: sha256WithRSAEncryption

         99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:

         b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:

         07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
         33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:

         c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:

         af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:

         7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:

         61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:

         0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:

         d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:

         3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:

         88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:

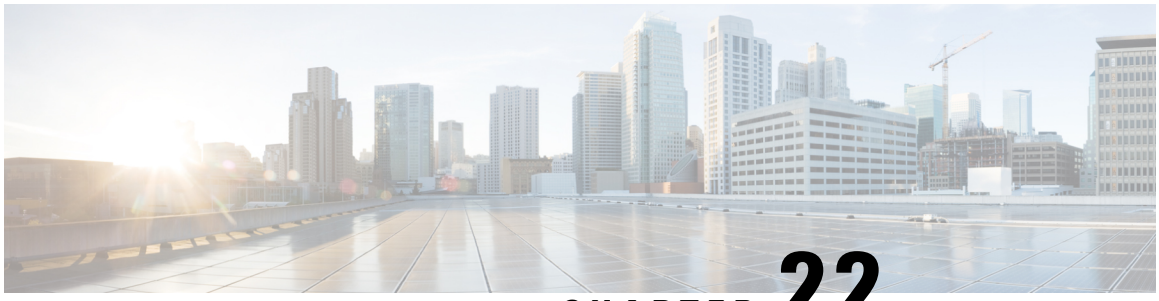
         19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:

         06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:

         2f:31:02:59


Device#
```

On a Cisco vEdge device, you can obtain a similar output by executing the command **show certificate reverse-proxy**.



CHAPTER 22

Onboarding Modular Cisco ASR 1000 Series Platforms

- Cisco ASR 1006-X with an RP3 Module, on page 397
- Information About the Cisco ASR 1006-X with an RP3 Module, on page 397
- RMA Replacement of the Cisco ASR 1006-X Chassis, on page 399
- RMA Replacement of the Cisco RP3 Module, on page 403

Cisco ASR 1006-X with an RP3 Module

Table 89: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Support for the Cisco ASR 1006-X Platform with an RP3 Module	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	Starting from this release, Cisco Catalyst SD-WAN supports the Cisco ASR 1006-X platform with a Cisco ASR 1000 Series Route Processor 3 module installed.

Information About the Cisco ASR 1006-X with an RP3 Module

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, Cisco vManage Release 20.5.1

Last supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.x, Cisco Catalyst SD-WAN Control Components Release 20.12.x

Cisco Catalyst SD-WAN supports the Cisco ASR 1006-X platform with a Cisco ASR 1000 Series Route Processor 3 (Cisco ASR1000-RP3) module.

Note Cisco Catalyst SD-WAN supports this configuration only when the Cisco ASR 1006-X and RP3 module are ordered as a unit for operation with Cisco Catalyst SD-WAN.

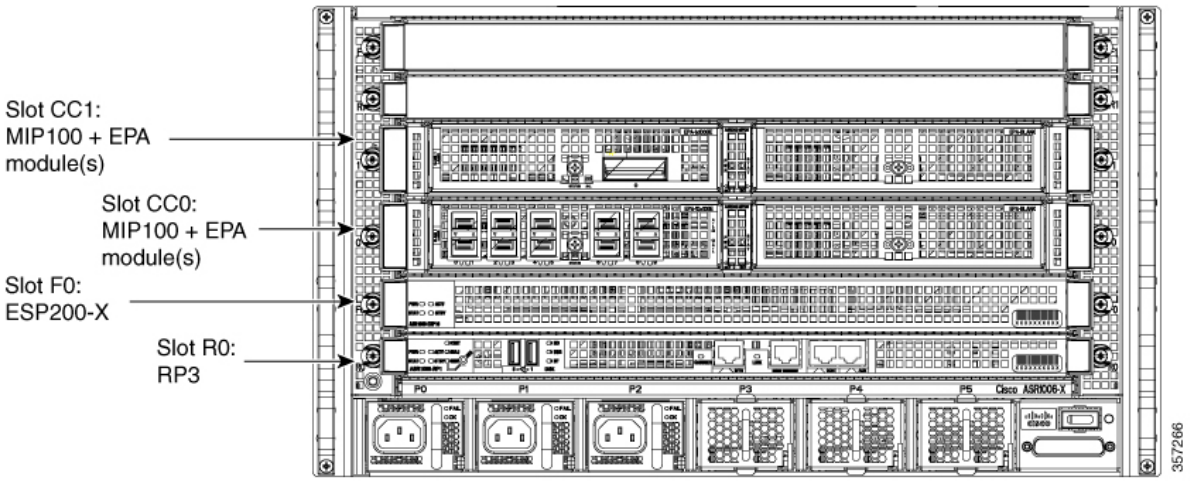
Hardware Configuration

The Cisco ASR 1006-X operates with Cisco Catalyst SD-WAN in the following configuration.

Table 90: Hardware Configuration

ASR 1006-X Slot	Contents
R0	Cisco ASR 1000 Series Route Processor 3 (Cisco ASR1000-RP3) module
F0	Cisco ASR 1000 Series 200-Gbps Embedded Services Processor (ASR1000-ESP200-X)
CC0	Cisco ASR1000-MIP100 carrier card + 1 or 2 EPA cards in the subslots of the carrier **Note** See below for supported EPA cards. When using only one EPA card in the carrier, you can place the EPA card in either subslot.
CC1	Cisco ASR1000-MIP100 carrier card + 1 or 2 EPA cards in the subslots of the carrier **Note** See below for supported EPA cards. When using only one EPA card in the carrier, you can place the EPA card in either subslot.
R1	This slot must be empty.
F1	This slot must be empty.

Figure 28: Cisco ASR 1006-X Slots and Modules



For information about installing the ASR1000-MIP100 carrier card and EPA cards, see the Cisco ASR 1000 Series Modular Interface Processor Hardware Installation Guide.

Supported Cards and Modules

The following Ethernet port adapter (EPA) cards are supported. Each ASR1000-MIP100 carrier card supports two EPA cards, and you can install a total of up to four EPA cards.

- 10-port 10 Gigabit Ethernet (10x10G):

  EPA-10X10GE

- 2-port 40 Gigabit Ethernet (2x40G):

  EPA-2X40GE

- 1-port 100 Gigabit Ethernet (1x100G):

  EPA-QSFP-1X100GE

Notes and Limitations

- **Hardware redundancy**

  Use only one ASR1000-RP3 and one ASR1000-ESP200-X, as described in the Hardware Configuration table above. Dual RP module or dual ESP hardware redundancy is not supported for the Cisco ASR 1006-X in this Cisco Catalyst SD-WAN use-case.

- **ISSU and OIR**

  The modules and cards do not support in-service software upgrade (ISSU) or online insertion and removal (OIR).

ROM Monitor Software Version

- For the Cisco ASR 1006-X platform, there are no specific ROM monitor (ROMmon) version requirements.
- The RP3 module requires ROM monitor (ROMmon) software version 16.9(5r) or later.

Onboarding Workflow

1. Verify that the Cisco ASR 1006-X meets the requirements described in Hardware Configuration and ROM Monitor Software Version.
2. Follow the Plug and Play onboard procedures described in the Cisco Plug and Play Support Guide for Cisco SD-WAN Products.
3. Follow the Cisco Catalyst SD-WAN onboarding procedure described in Plug and Play Onboarding Workflow.

RMA Replacement of the Cisco ASR 1006-X Chassis

Use this procedure if it is necessary to replace the Cisco ASR 1006-X chassis as part of a return material authorization (RMA) process. This procedure replaces the Cisco ASR 1006-X chassis, but keeps the current cards (RP3 module, ESP200 module, MIP100 carrier cards, EPA cards).

Before You Begin

- The Cisco ASR 1006-X (which is now faulty) with an RP3 module has been fully onboarded in Cisco SD-WAN Manager.
- Make note of the following serial numbers:
  - Replacement Cisco ASR 1006-X chassis serial number
  - Certificate serial number for the RP3 module
  - SUDI serial number for the RP3 module

Replace the Cisco ASR 1006-X Chassis

To replace the Cisco ASR 1006-X chassis, perform the following steps.

Note In tables listing devices, Cisco SD-WAN Manager does not distinguish between the Cisco ASR 1006-X chassis and the RP3 module installed in the chassis. A single row in the table shows the combined information for both.

1. (Perform this step only if you have applied a feature template to the current device (which is now faulty), and if you want to save the existing configuration to use it on the replacement device.)

   Save the device settings file for the RP3 module.

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

   b. Click **Device Templates**.

   Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

   c. Click **…** for the template that is attached to the Cisco ASR 1006-X containing the RP3 module, and choose **Export CSV** to download the device settings CSV file.

2. In the Cisco Plug and Play (PnP) Connect web portal, remove the current Cisco ASR 1006-X chassis.

   Note The PnP Connect web portal is linked to Cisco commerce workspace (CCW), facilitating automatic registration of the serial numbers and PIDs of purchased devices in the PnP Connect web portal. For more information see the Cisco Plug and Play Support Guide for Cisco SD-WAN Products, and the RMA topic in the Cisco Network Plug and Play Connect Capability Overview.

   Note The functionality of the PnP Connect web portal is subject to change, and is outside the scope of this document. For additional details, see the PnP Connect web portal documentation.

In the PnP Connect web portal, use **Devices** > **Delete Selected Device**, or the equivalent, to remove the current Cisco ASR 1006-X chassis.

3. In the Cisco Plug and Play (PnP) Connect web portal, add the replacement Cisco ASR 1006-X chassis.
   a. In the PnP Connect web portal, choose **Devices** > **Add Device**, or the equivalent, and select the option to enter new device details.
   b. Enter the serial number for the replacement Cisco ASR 1006-X chassis.



Note You can use the **show pnp version** command on the Cisco ASR 1006-X router to display the serial number.

   c. Add the SUDI serial number and certificate serial number of the RP3 module.



Note If the RP3 module is mounted in a working chassis, you can use the **show sdwan certificate serial** command to display these serial numbers.

   d. Save the update.

4. Remove the entry for the current Cisco ASR 1006-X chassis in Cisco SD-WAN Manager.
   a. In Cisco SD-WAN Manager, detach the current device template from the current Cisco ASR 1006-X chassis.
   b. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
   c. In the row with the current Cisco ASR 1006-X, in the **Validate** column, click **Invalid**, and **OK**.

      The task view indicates when the process is complete.
   d. Click **Send to Controllers**.
   e. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   f. In the row with the current Cisco ASR 1006-X, click **More Options** (**…**) and choose **Delete WAN Edge**.

5. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** and click **Sync Smart Account**.

   Cisco SD-WAN Manager loads the details of the replacement Cisco ASR 1006-X chassis from your Smart Account.

6. If you saved a CSV file in an earlier step, edit the file to update it with the device ID of the replacement chassis.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
   b. Copy device ID of the new chassis from the **Chassis Number** column in the device list.
   c. Open the CSV file in a text editor or spreadsheet application, and edit the csv-deviceId value in the first column, updating it to use the device ID of the new chassis.

7. Attach a device template to the replacement Cisco ASR 1006-X. Use the same device template that was used for previous chassis. If you saved a CSV file in an earlier step, use it in the substeps that follow.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

   c. In the row of the template that was previously attached to the current chassis, click **More Actions** (**…**) and choose **Attach Devices**.
   d. In the **Available Devices** pane, select the replacement chassis and move it to the **Selected Devices** pane.
   e. Click **Attach**. The **Configuration Templates** page opens.
   f. If you saved a CSV file in an earlier step, click the **up arrow** button to upload a CSV file.
   g. If you saved a CSV file in an earlier step, in the **Upload CSV File** pop-up window, select the CSV file edited in a previous step, and click **Upload**. The values stored in the CSV file are copied to the device template.
   h. Click **Next**.
   i. Click **Configure Devices** to push the device template to the replacement Cisco ASR 1006-X chassis. The task status shows this task as Scheduled because the replacement device is not yet reachable.
8. Save the device configuration file.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
   b. In the row of the Cisco ASR 1006-X, click **More Options** (**…**) and choose **Generate Bootstrap Configuration**.
   c. In the pop-up window, click the **Cloud-Init** radio button.
   d. Click **Download** to download the configuration file.
   e. Rename the downloaded file to: ciscosdwan.cfg
9. Copy the bootstrap file (ciscosdwan.cfg) created in an earlier step, to a USB flash drive, and plug this into the current RP3 module.
10. If the current Cisco ASR 1006-X chassis is still operating, power it down.
11. Remove the modules and cards (RP3 module, ESP200 module, MIP100 carrier cards, EPA cards) from the current Cisco ASR 1006-X chassis.
12. Connect the USB flash drive, which has the configuration file saved in an earlier step, to the RP3 module.
13. Install the modules and cards in the new Cisco ASR 1006-X chassis.

    For information about RP3 module installation, see the Cisco ASR 1000 Route Processor 3 Installation and Configuration Guide.

For information about MIP100 and EPA installation, see the Cisco ASR 1000 MIP and EPA Hardware Installation Guide.

14. Power up the replacement Cisco ASR 1006-X router.
15. After the router is powered up, execute the **controller-mode reset** command on the router to reset the RP3 module.

    When the RP3 module starts, the following occurs:

    - The RP3 module loads the configuration from the ciscosdwan.cfg file on the USB flash drive.
    - The RP3 module boots up in controller mode.



Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, controller mode is not supported.

    - When the connection to the controller is established, the controller pushes the device template, which was in Scheduled state, to the RP3 module.

RMA Replacement of the Cisco RP3 Module

Use this procedure if it is necessary to replace the RP3 module used with the Cisco ASR 1006-X as part of a return material authorization (RMA) process.

Prerequisites

- The Cisco ASR 1006-X with an RP3 module (which is now faulty) has been onboarded in Cisco SD-WAN Manager.
- Make note of the following serial numbers:
    - Cisco ASR 1006-X chassis serial number
    - Certificate serial number for the replacement RP3 module
    - SUDI serial number for the replacement RP3 module

Replace the Cisco RP3 Module

To replace the Cisco RP3 module, perform the following steps.



Note In tables listing devices, Cisco SD-WAN Manager does not distinguish between the Cisco ASR 1006-X chassis and the RP3 module installed in the chassis. A single row in the table shows the combined information for both.

1. (Perform this step only if you have applied a feature template to the current device (which is now faulty), and if you want to save the existing configuration to use it on the replacement device.)

Save the device settings file for the RP3 module.

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

c. Click **More Options** (**…**) for the template that is attached to the Cisco ASR 1006-X containing the RP3 module, and choose **Export CSV** to download the device settings CSV file.

2. Save the device configuration file for the RP3 module.

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.

b. In the row for the Cisco ASR 1006-X containing the RP3 module, click **More Options** (**…**) and choose **Generate Bootstrap Configuration**.

c. In the pop-up window, click the **Cloud-Init** radio button.

d. Click **Download** to download the configuration file.

e. Rename the downloaded file to: ciscosdwan.cfg

3. In the Cisco Plug and Play (PnP) Connect web portal, update the SUDI serial number and certificate serial number within the Cisco ASR 1006-X entry, to use the serial numbers of the replacement RP3 module.

Note The PnP Connect web portal is linked to Cisco commerce workspace (CCW), facilitating automatic registration of the serial numbers and PIDs of purchased devices in the PnP Connect web portal. For more information see the Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products, and the RMA topic in the Cisco Network Plug and Play Connect Capability Overview.

Note The functionality of the PnP Connect web portal is subject to change, and is outside the scope of this document. For additional details, see the PnP Connect web portal documentation.

a. In the PnP Connect web portal, choose **Devices** > **Edit Device** and select the Cisco ASR 1006-X entry for the device that contains the RP3 module that is being replaced.

b. In the Cisco ASR 1006-X entry, delete the SUDI serial number and certificate serial number of any existing RP3 module entries (there may be more than one).

c. Add the SUDI serial number and certificate serial number for the replacement RP3 module.

d. Save the update.

4. In Cisco SD-WAN Manager, remove the current RP3 module and add the replacement RP3 module.

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

b. In the row with the Cisco ASR 1006-X device containing the RP3 module, in the **Validate** column, click **Invalid**, and **OK**.

The task view indicates when the process is complete.

c. Click **Send to Controllers**.

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

e. In the row with the Cisco ASR 1006-X device containing the RP3 module, click **More Options** (**…**) and choose **Delete WAN Edge**.

f. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** and click **Sync Smart Account**.

Cisco SD-WAN Manager loads the details of the replacement RP3 module. At this point, before you have physically replaced the RP3 module, the device table shows the following in the row of the Cisco ASR 1006-X device:

- Device Model: ASR1006-X
- Chassis Number: No change to the chassis number
- Serial No./Token: Updated to show the serial number of the replacement RP3 module, as loaded from the Smart Account

5. Attach a device template to the replacement Cisco ASR 1006-X. Use the same device template that was used for previous chassis. If you saved a CSV file in an earlier step, use it in the substeps that follow.

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b. Click **Device Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

c. In the row of the template that was previously attached to the current chassis, click **More Actions** (**…**) and choose **Attach Devices**.

d. In the **Available Devices** pane, select the replacement chassis and move it to the **Selected Devices** pane.

e. Click **Attach**. The **Configuration Templates** page opens.

f. If you saved a CSV file in an earlier step, click the **up arrow** button to upload a CSV file.

g. If you saved a CSV file in an earlier step, in the **Upload CSV File** pop-up window, select the CSV file and click **Upload**. The values stored in the CSV file are copied to the device template.

h. Click **Next**.

i. Click **Configure Devices** to push the device template to the replacement Cisco ASR 1006-X chassis. The task status shows this task as Scheduled because the replacement device is not yet reachable.

6. Copy the bootstrap file (ciscosdwan.cfg) created in an earlier step, to a USB flash drive, and plug this into the replacement RP3 module.

7. Remove the previous RP3 module from the Cisco ASR 1006-X chassis, and install the replacement RP3 module.

   For information about RP3 module installation, see the Cisco ASR 1000 Route Processor 3 Installation and Configuration Guide.

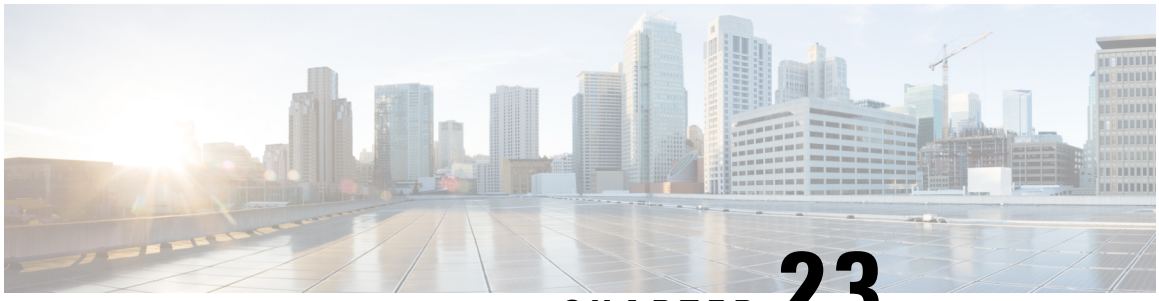
   When the RP3 module starts, the following occurs:

   - The RP3 module loads the configuration from the ciscosdwan.cfg file on the USB flash drive.
   - The RP3 module boots up in controller mode.



Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, controller mode is not supported.

   - When the connection to the controller is established, the controller pushes the device template, which was in Scheduled state, to the RP3 module.



CHAPTER 23

Getting started with the SD-WAN Manager API

- SD-WAN Manager APIs, on page 407

SD-WAN Manager APIs

SD-WAN Manager API is a Representational State Transfer Application Programming Interface (REST API) that is used for:

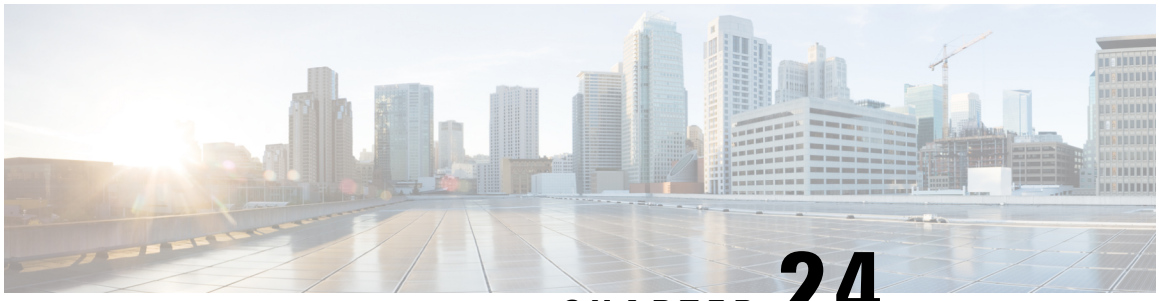
- controlling, configuring, and monitoring the Cisco devices in an overlay network, and
- enabling clients to utilize the features provided by SD-WAN Manager.

Use cases

Some of the use cases for SD-WAN Manager API are:

- Provisioning: Streamline manual tasks with automation. APIs enable the automated provisioning of Cisco Catalyst SD-WAN overlays, eliminating the need for network administrators to manually configure routers, routing, security policies, or other SD-WAN features. Organizations can utilize provisioning platforms or automation tools, laying the groundwork for Network as Code.
- Network visibility: APIs enhance network visibility by allowing seamless integration with monitoring tools to collect and analyze network performance data. They provide insights into network traffic, device status, and potential issues, enabling proactive management and troubleshooting.
- Integration with third-Party tools: Enhance API integration with external network management and monitoring solutions to offer a more comprehensive view of the network environment.
- Network as Code: Leverages APIs from Cisco Catalyst SD-WAN Manager to automate network configuration and management, treating network infrastructure as programmable assets. This approach enables streamlined deployment, consistent configuration, and rapid adaptation to changes, enhancing efficiency and reducing errors.

For more information, see Cisco Catalyst SD-WAN Manager API Guide.



CHAPTER 24

Deploy Cisco SD-WAN Controller in Microsoft Azure

Table 91: Feature History

Feature Name	Release Information	Description
Deploy Cisco SD-WAN Controllers in Azure	Cisco vManage Release 20.6.1	This feature enables you to deploy the Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco Catalyst SD-WAN Validator) in a Microsoft Azure environment.

- Information About Deploying Cisco SD-WAN Controllers in Azure, on page 409
- Prerequisites for Deploying Cisco SD-WAN Controllers in Azure, on page 410
- Use Cases for Deploying Cisco SD-WAN Controllers in Azure, on page 411
- Deploy Cisco SD-WAN Controllers in Azure: Tasks, on page 411
- Verify the Deployment of Cisco SD-WAN Controllers in Azure, on page 416
- Monitor the Deployment of Cisco SD-WAN Controllers in Azure, on page 417

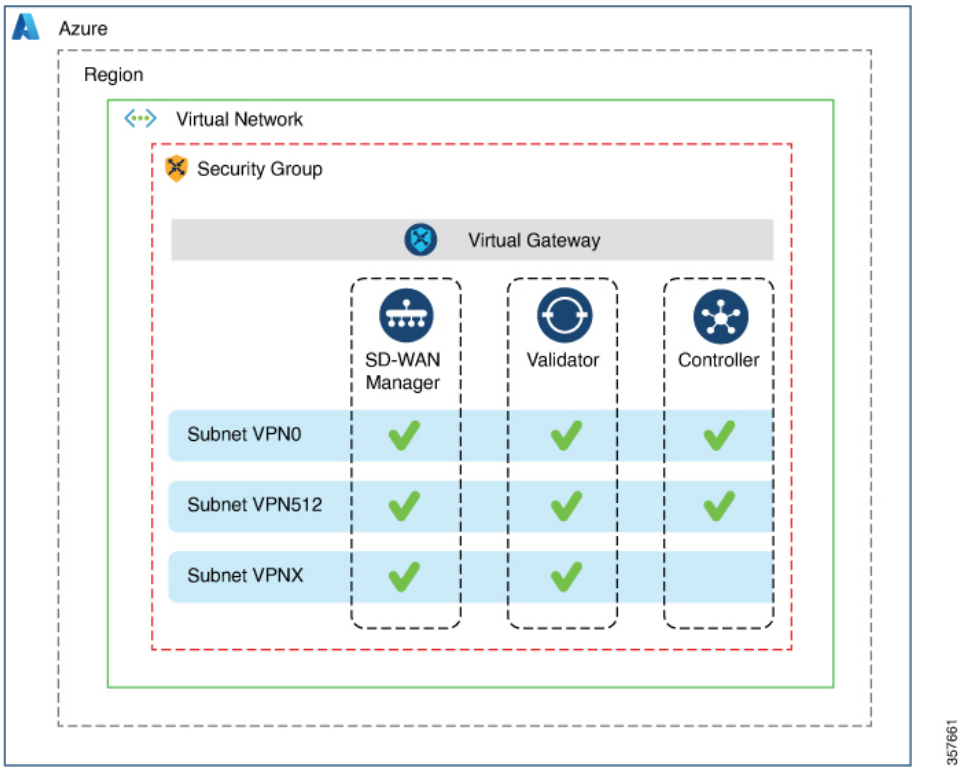
Information About Deploying Cisco SD-WAN Controllers in Azure

Minimum supported controller images: Cisco vManage Release 20.6.1, Cisco Catalyst SD-WAN Control Components Release 20.6.1, and Cisco SD-WAN Validator Release 20.6.1

You can deploy the following Cisco SD-WAN Controllers in an Azure environment: Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.

The following illustration shows the architecture of the Azure region, virtual network, security group, and so on, and it shows where the Cisco SD-WAN Controllers function within the architecture.

Figure 29: Cisco SD-WAN Controllers in Azure



Benefits of Deploying Cisco SD-WAN Controllers in Azure

- Set-up cost: Requires low initial set-up cost, as compared with on-premises hosting, as there is no requirement to purchase additional data center infrastructure
- Deployment: Ease of cloud-based deployment
- Management: Ability to manage devices worldwide
- Stability: Because of its reliability, Azure hosting provides a stable environment for Cisco SD-WAN Controllers.
- Security: Azure provides a secure hosting environment.
- Scaling: Azure provides an easy path to increasing the scale of your Cisco Catalyst SD-WAN network.

Prerequisites for Deploying Cisco SD-WAN Controllers in Azure

You must have a valid (and active) Microsoft Azure subscription.

Use Cases for Deploying Cisco SD-WAN Controllers in Azure

For a Cisco Catalyst SD-WAN deployment that is already using Azure, such as for Cisco Catalyst 8000V Edge Software, hosting the Cisco SD-WAN Controllers in Azure is a logical, efficient choice, keeping all services in alignment.

Deploy Cisco SD-WAN Controllers in Azure: Tasks

Note The procedures described here apply to the three types of Cisco SD-WAN Controllers— Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator. Where applicable, we indicate where the instructions are different for specific controllers.

Note In DHCP configurations, IPv6 Unique Local Addresses (ULA) are assigned to the interface in some instances. Cisco SD-WAN Validator is designed to drop the packets with source or destination as the ULA addresses. In an Azure setup, to allow packets with these addresses on the device, configure the **enable-ipv6-unique-local-address** command to enable or disable these addresses.

Task 1: Create a Controller Image in Azure

Before You Begin

On the Cisco Software Download page, download the images for the Cisco SD-WAN Control Components: Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator. Decompress the downloaded files, which are in .tar format. The image file for each controller is in virtual hard disk (VHD) format.

Create a Controller Image in Azure

Note For definitive information about tasks in Azure, see the Azure documentation.

Perform the following steps in the Azure portal:

1. If you do not already have a storage account in Azure, create one now.
   - Provide a name, location, and so on, for the storage account.
   - For network connectivity, use the default options for connectivity method, routing preference, data protection, and secure transfer.
   - Optionally, you can enter a tag to categorize the storage account.

2. Create a new private container in the storage account. Choose a storage account in the region where you intend to deploy the controller.

Note Each controller requires a separate container.

3. Upload the VHD file of the controller into the container.

   During the upload procedure, choose Page Blob for the blob type.

Note For information about choosing the blob type, see Azure documentation.

4. Create a new image, selecting the VHD file uploaded in the previous step.

   When creating an image, ensure that you complete the following actions:

   - Choose a valid subscription.
   - Choose an existing resource group or create a new one.
   - Enter a name and region for the image.
   - For OS, choose Linux.
   - For VM generation, choose Gen 1.
   - For account type, choose Premium SSD.
   - For host caching, choose read/write
   - For encryption, choose the default settings.
   - Optionally, you can enter a tag to categorize the image.

Task 2: Create a Virtual Network, Subnets, and Network Security Group in Azure

Note For definitive information about tasks in Azure, see the Azure documentation.

Perform the following steps in the Azure portal:

1. Begin the workflow for creating a virtual network.

   When creating a virtual network, ensure that you complete the following actions:

   - Choose a valid subscription.
   - Choose an existing resource group or create a new one.

Note A resource group is a logical construct in Azure that includes all of the resources that you have deployed across regions. We recommend defining one resource group for each Cisco Catalyst SD-WAN overlay.

- Enter a name and region for the virtual network.
- Enter an address space for the virtual network.

  Example: 10.0.0.0/16
- Add a minimum of two subnets to the virtual network, and an additional subnet if you are using a Cisco SD-WAN Manager cluster. For each subnet, provide a name and an address space for the subnet. A later step associates these subnets with VM network interfaces.

  Example:

  10.0.1.0/24
  10.0.2.0/24
  10.0.3.0/24
- Optionally, you can enter a tag to categorize the virtual network.

2. Begin the workflow for creating a network security group (NSG).

   When creating a network security group, ensure that you complete the following actions:
   - Choose a valid subscription.
   - Choose the resource group created in the previous step, as part of the workflow for creating a virtual network.
   - Enter a name and region for the NSG.
   - Optionally, you can enter a tag to categorize the NSG.
3. Associate the newly created NSG with the subnets created in an earlier step.

Task 3: Create a Virtual Machine for the Controller

Note For definitive information about tasks in Azure, see the Azure documentation.

Perform the following steps in the Azure portal:

1. Begin the workflow for creating a virtual machine (VM).

   When creating a VM, ensure that you complete the following actions:
   - Deploy the VM in the virtual network created in Task 2.
   - Select the resource group that you created in a previous task, during the workflow for creating a virtual network.

- Enter a name and region for the VM.
- For the image, select the uploaded controller image.



Note For information about how to locate custom images, see the Azure documentation.

- For the VM size, select an option with the number of CPUs and memory that you want to use for the controller.

  For information about Cisco SD-WAN Controller-device compatibility and server requirements, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.
- Choose an authentication type (for example, SSH public key, or password) and provide the credentials, as required.
- For disk resources, do one of the following:
  - If you are deploying a Cisco Catalyst SD-WAN Controller or a Cisco Catalyst SD-WAN Validator, no additional disk resources are required beyond the default.
  - If you are deploying a Cisco SD-WAN Manager controller, choose one disk.
    - Choose the Premium SSD option and default encryption.
    - Choose a disk size of 1 TiB (called P30 in Azure) or larger.

      For server recommendations relevant to controllers in Azure, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.
    - Configure the disk host caching as read/write.
- For networking details, choose the virtual network, the subnets, and the NSG that you created in earlier steps.
- For the public IP address, choose the following options:
  - SKU: Basic
  - Assignment: static



Note Cisco Catalyst SD-WAN requires a static IP address for controllers.

- Optionally, you can enable advanced boot diagnostics (a management option) to create an additional storage account in the resource group for storing diagnostics logs.
- (Controller releases 20.6.1 and later) Optionally, you can use the custom data feature (an advanced option) to enter commands for the VM to execute when rebooting.
- Optionally, you can add a tag to categorize the controller.

2. After creating the VM, create additional network interfaces (NICs) for the VM.

Create the network interfaces in the resource group that you created in an earlier task.

- If you are deploying a Cisco SD-WAN Controller or Cisco SD-WAN Validator, create one additional network interface.
- If you are deploying a Cisco SD-WAN Manager controller, create two additional network interfaces.
- If you are deploying a Cisco SD-WAN Manager controller in a cluster, see Cluster Management and Deploy Cisco Catalyst SD-WAN Manager for additional information about Cisco SD-WAN Manager out-of-band interfaces.

When creating a network interface, ensure that you complete the following actions:

- Specify the virtual network, subnets, and NSG created in earlier tasks.
- Associate NIC 1 with subnet 1.

  If you are deploying a Cisco SD-WAN Manager controller, associate NIC 2 with subnet 2.

  If you are using a Cisco SD-WAN Manager cluster, associate NIC 3 with subnet 3.



Note Associating a NIC with a subnet enables the VM to connect to the subnet.

- For each NIC, enter the tag used for the controller that you are deploying.

3. Create a static public IP for all of the controllers to use, and associate this public IP with NIC 1.



Note Use the IP configurations option in Azure to create the public IP.

When creating a public IP, ensure that you complete the following actions:

- For assignment, choose static.
- Use the associate option to specify NIC 1.

4. Stop the VM, and confirm when it has stopped.
5. Attach the newly created NICs to the VM.
   - If you are deploying a Cisco SD-WAN Controller or Cisco SD-WAN Validator, attach the NIC to the VM.
   - If you are deploying Cisco SD-WAN Manager, attach both of the newly created NICs to the VM.
6. Restart the VM.

   Confirm in the Azure portal that the VM has restarted.

Task 4: Configure the Network Security Group

Before You Begin

The NSG is related functionally to firewall policy. When configuring the NSG, it is helpful to be aware of firewall port configuration in Cisco Catalyst SD-WAN. For more information on firewall ports, see Firewall Ports for Cisco SD-WAN Deployments.

Configure the Network Security Group

Note For definitive information about tasks in Azure, see the Azure documentation.

1. Using the Azure portal, add inbound security rules to the NSG created in an earlier task, to allow inbound traffic from the IP ranges needed for the following:
   - Establishing control connections between each of the Cisco SD-WAN Controller. If the controllers lack connectivity to each other, the control plane and data plane cannot operate.
   - Accessing the controllers using HTTPS or SSH protocols.

   For the NSG, use the option to add inbound security rules. Using the rules, allow all of the controller VM IP addresses, to enable the required connectivity between the Cisco SD-WAN Controller.

   When creating a new inbound security rule, ensure that you complete the following actions:
   - Specify IP ranges, protocol, and so on.
   - For the action of the rule, choose the option to allow the traffic.
2. To verify connectivity, log in to the VM using the NIC 0 public IP of Cisco SD-WAN Manager.

Verify the Deployment of Cisco SD-WAN Controllers in Azure

- Infrastructure:

  To verify the deployment of Cisco SD-WAN Controllers within virtual machines in Azure, use the Azure portal to check that the VMs hosting each controller are active.

- Services:

  To verify that Cisco Catalyst SD-WAN services are operating after deployment of the controllers, use the following steps:

  1. Check for a successful ping to the VM that hosts Cisco SD-WAN Manager.
  2. Log in to Cisco SD-WAN Manager.
  3. Use SSH to connect to Cisco SD-WAN Manager, and use the **request nms all status** command. The output shows the status of all of the Cisco SD-WAN Manager services. Confirm that the application server is active.

The following excerpt of the **request nms all status** command output shows that the application server is active:

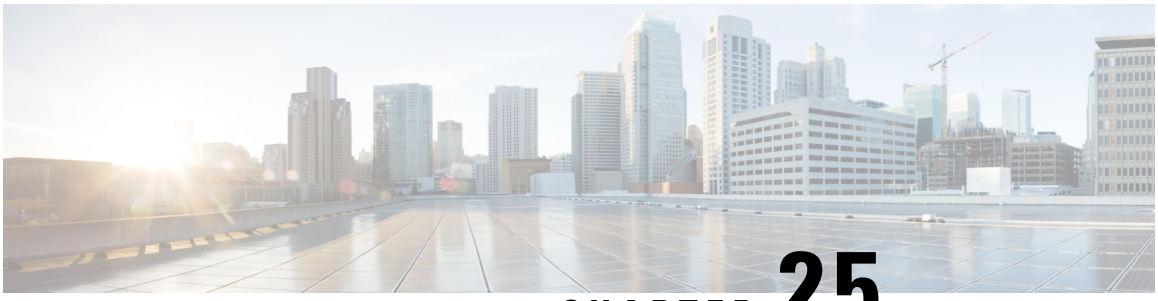
```
vmanage# request nms all status
NMS service proxy
        Enabled: true
        Status: running PID:2881 for 9479s
NMS service proxy rate limit
        Enabled: true
        Status: running PID:4359 for 9521s
NMS application server
        Enabled: true
        Status:  running PID:6131 for 9419s
...
```

4. After installing the controllers, follow the steps in Cisco SD-WAN Overlay Network Bring-Up Process to establish the control connections for the controllers and to verify that each controller is operational.

Monitor the Deployment of Cisco SD-WAN Controllers in Azure

To monitor infrastructure status, such as CPU usage and disk usage, use the monitoring tools in the Azure portal.

For information about monitoring the status of Cisco Catalyst SD-WAN services, see the Cisco SD-WAN Monitor and Maintain guide.



CHAPTER 25

Deploy Cisco SD-WAN Controllers in the AWS Cloud

Table 92: Feature History

Feature Name	Release Information	Description
Deploy Cisco SD-WAN Controllers in AWS	Cisco vManage Release 20.6.1	This feature enables you to deploy the Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco SD-WAN Validator) in an Amazon AWS environment.

- Information About Deploying Cisco SD-WAN Controllers in AWS, on page 419
- Prerequisites for Deploying Cisco SD-WAN Controllers in AWS, on page 421
- Use Cases for Deploying Cisco SD-WAN Controllers in AWS, on page 421
- Deploy Cisco SD-WAN Controllers in AWS: Tasks, on page 421
- Verify the Deployment of Cisco SD-WAN Controllers in AWS, on page 426
- Monitor the Deployment of Cisco Catalyst SD-WAN Controller in AWS, on page 426

Information About Deploying Cisco SD-WAN Controllers in AWS

Minimum supported controller images: Cisco vManage Release 20.6.1, Cisco vSmart controller Release 20.6.1, and Cisco vBond orchestrator Release 20.6.1.

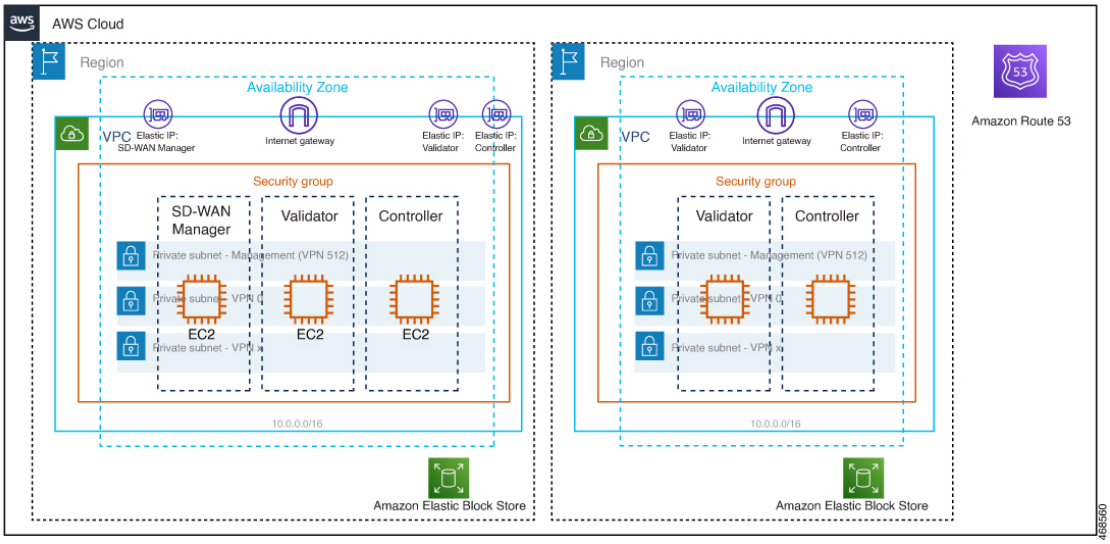
You can deploy the following Cisco SD-WAN Controllers in an Amazon Web Services (AWS) environment using Amazon Machine Images (AMI): Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.

The AMI images that Cisco provides to you are for your use only. Do not share them with others. You can do the following:

- You can deploy the number of controllers as per your order quantity. For example, if you have ordered 50 Cisco SD-WAN Manager controller PIDs, then you can deploy only 50 Cisco SD-WAN Manager controllers within your AWS account.
- You can copy the AMI between regions and your own separate AWS accounts, if you do not exceed the quantity of PIDs ordered.
- After the initial deployment of the controllers, you are responsible for any upgrades or downgrades.

The following illustration shows the architecture of the AWS region, virtual private cloud (VPC), security group, and so on, and it shows where the Cisco SD-WAN Controllers function within the architecture.

Figure 30: Cisco SD-WAN Controllers in AWS



Considerations Before Installing Cisco SD-WAN Controllers in AWS

- Cisco Catalyst SD-WAN controller AMIs are not available on the Cisco software download site or AWS marketplace. They are provided only when you request them with a valid business case to set up Cisco SD-WAN Controllers in your AWS cloud account.
- For information about ordering Cisco SD-WAN Controllers to use with AWS, contact your Cisco account team or Cisco partner.
- Cisco does not provide support for any issues that arise with the cloud infrastructure during the provisioning or installation of the controllers.
- Troubleshooting:
  - Functionality issues: Please open a Cisco TAC case for functionality issues.
  - Infrastructure issues: You are responsible for infrastructure management, monitoring, and troubleshooting. After the controllers are provisioned and running in your cloud account, Cisco does not provide support for cloud infrastructure-related issues.
- Software upgrade: Controller software upgrade doesn't require AMI images. You can download the controller images from the Cisco software download site and upgrade the controller software as described in the Manage Software Upgrade and Repository chapter of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Benefits of Deploying Cisco SD-WAN Controllers in AWS

- Set-up cost: Low initial set-up cost, as compared with on-premises hosting, as there is no requirement to purchase additional data center infrastructure.

- Deployment: Ease of cloud-based deployment.
- Management: Ability to manage devices worldwide.
- Stability: Because of its reliability, AWS hosting provides a stable environment for Cisco SD-WAN Controllers.
- Security: AWS provides a secure hosting environment.
- Scaling: AWS provides an easy path to increase the scale of your Cisco Catalyst SD-WAN network.

Prerequisites for Deploying Cisco SD-WAN Controllers in AWS

- You must have valid (and active) AWS and Cisco accounts.
- Contact your Cisco account team for PID information for ordering the appropriate controller PID for your cloud deployment.

Use Cases for Deploying Cisco SD-WAN Controllers in AWS

- Use case 1: For complete control of provisioning, management and monitoring of controllers and scalability using your own public cloud account.
- Use case 2: For specific architectural or security posture requirements.

Deploy Cisco SD-WAN Controllers in AWS: Tasks



Note The procedures described here apply to the three types of Cisco SD-WAN Controllers—Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator. We indicate the difference in the instructions for specific controllers wherever applicable.

Task 1: Request AWS AMI Images

You can deploy Cisco SD-WAN Controllers in an AWS account using AMI images.

1. You must place an order for $0 customer managed Cisco Catalyst SD-WAN Controller SKU. For more information, refer section 2.3 SKU Table in the Cisco Catalyst SD-WAN Controller Ordering Guide.
2. After you purchase the SKU, the Cisco CloudOps team validates the order information, and reach out to the customer asking for additional details such as:
   a. AWS account number.
   b. Software version requirement for the AMI.

3. Cisco CloudOps team verifies the information and shares the requested AMIs to your AMI inventory in the US-WEST-2 region.

Note The AMI images that the CloudOps team provides are for your use only. Do not share them with others. If the images are shared with others, Cisco reserves the right to remove the images and take any necessary action to prevent the images from being shared.

Task 2: Create a VPC, Subnet, and Security Group in AWS

Note For definitive information about tasks in AWS, see the AWS documentation.

Perform the following steps in the AWS portal:

1. Create a virtual private cloud (VPC), and while creating the VPC ensure that you complete the following actions:
   - Enter a name and a region for the VPC.
   - Enter an address space for the VPC. Example: 10.0.0.0/16
   - Add a minimum of two subnets to the VPC, and an additional subnet if you plan to create a Cisco SD-WAN Manager cluster. For each subnet, provide a name and an address space for the subnet. A later step associates these subnets with virtual machine network interfaces.

     Example:
     - Add subnet 0 with the address 10.0.1.0/24, which will be VPN 512 used as the primary interface for the controllers.
     - Add subnet 1 with the address 10.0.2.0/24, which will be used as the controllers' transport or tunnel interface for VPN 0.
     - Add subnet 2 with the address 10.0.3.0/24, which will be for used for Cisco SD-WAN Manager clustering (only if you are needed in case of deploying a Cisco SD-WAN Manager cluster).
   - (Optional) Enter a tag to categorize the VPC.
2. Create the necessary resources required for the VPC, to form the environment for running the controller instances:
   - The security group must contain the following:
     - Source public IP address of the user NOC center to access the controllers for management purpose.
     - Address 0.0.0.0/0 for all TCP/UDP ports for TLS/DTLS for all edges to join the controllers.
     - Enable public IPs each controller to reach other controllers.
   - Enter a name and a region for the security group.

- (Optional) Enter a tag to categorize the security group.

3. Associate the newly created security group with the subnets created in Step 1.
4. Create an internet gateway and associate it with the VPC.
5. Create a routing table and associate it with the VPC. Add a default route entry pointing to the internet gateway.

Task 3: Create a Virtual Machine for the Controller

Note For definitive information about tasks in AWS, see the AWS documentation.

Perform the following steps in the AWS portal:

1. Begin the workflow for creating a virtual machine. When creating a virtual machine, ensure that you complete the following actions:
   - Deploy the virtual machine in the virtual private cloud (VPC) created in Task 2.
   - Enter a name and region for the virtual machine.
   - For the image, select the appropriate shared controller AMI for Cisco SD-WAN Manager or Cisco SD-WAN Validator or Cisco SD-WAN Controller.

Note For information about how to locate custom images, see the AWS documentation.

   - For the virtual machine size, select an option with the number of CPUs and memory that you want to use for the controller. For Cisco SD-WAN Controller-device compatibility and Cisco SD-WAN Controller server requirements, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.
   - Choose an authentication type (for example, SSH public key, or password) and provide the credentials, as required.
   - For disk resources, perform one of the following:
     - If you are deploying a Cisco SD-WAN Controller or a Cisco SD-WAN Validator, no additional disk resources are required beyond the default.
     - If you are deploying a Cisco SD-WAN Manager controller, choose one disk.
       - Choose the Premium SSD option and default encryption.
       - Choose a disk size of 1 TB (General Purpose SSD gp2) or larger.

         For server recommendations relevant to controllers in AWS, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.
       - Configure the disk host caching as read/write.

- For networking details, choose the VPC, the subnets, and the security group that you created in earlier steps. Each virtual machine must have two network interfaces, one for the VPN 512 management subnet and one for the VPN 0 tunnel subnet.
- Assign an Elastic IP address to the VPN 0 and VPN 512 network interfaces of each controller.
- (Optional) Enable advanced boot diagnostics (a management option) to create an additional storage account in the resource group for storing diagnostics logs.
- For Cisco SD-WAN Controller Release 20.6.1 and later, you can optionally use the custom data feature to enter commands for the virtual machine to execute when rebooting.
- (Optional) Add a tag to categorize the controller.

2. After creating the virtual machine, create additional network interfaces (NICs) for the virtual machine. Create the network interfaces in the resource group that you created in an earlier task.
   - If you are deploying a Cisco SD-WAN Controller or Cisco SD-WAN Validator, create one additional network interface.
   - If you are deploying a Cisco SD-WAN Manager controller, create two additional network interfaces.
   - If you are deploying a Cisco SD-WAN Manager controller in a cluster, see Cluster Management and Deploy Cisco SD-WAN Manager for additional information about Cisco SD-WAN Manager out-of-band interfaces.
3. When creating a network interface, ensure that you complete the following actions:
   - Specify the VPC, subnets, and the security group created in Task 2.
   - Associate NICs with subnets.

     Example: Associate NIC 1 with subnet 1.
     - If you are deploying a Cisco SD-WAN Manager controller, associate NIC 2 with subnet 2.
     - If you are using a Cisco SD-WAN Manager cluster, associate NIC 3 with subnet 3.



Note Associating a NIC with a subnet enables the virtual machine to connect to the subnet.

   - For each NIC, enter the tag used for the controller that you are deploying.
4. Create a static public IP for all the controllers to use, and associate this public IP with NIC 1.



Note Use the IP configuration option in AWS to create the public IP.

5. When creating a public IP, ensure that you complete the following actions:
   - For assignment, choose static.

- Use the associate option to specify NIC 1.

6. Stop the virtual machine, and confirm when it has stopped.
7. Attach the newly created NICs to the virtual machine.
   - If you are deploying a Cisco SD-WAN Controller or Cisco SD-WAN Validator, attach the NIC to the virtual machine.
   - If you are deploying Cisco SD-WAN Manager, attach both of the newly created NICs to the virtual machine.
8. Restart the virtual machine. Confirm in the AWS portal that the virtual machine has restarted.

Task 4: Configure the Security Group

Before You Begin

The security group is functionally related to a firewall policy. When configuring the security group, it is helpful to be aware of firewall port configuration in Cisco Catalyst SD-WAN. See Firewall Ports for Cisco SD-WAN Deployments.

Note For definitive information about tasks in AWS, see the AWS documentation.

Configure the Security Group

1. Using the AWS portal, add inbound security rules to the security group created in an earlier task, to allow inbound traffic from the IP range required for the following:
   - Establishing control connections between each of the Cisco SD-WAN Controllers. If the controllers lack connectivity to each other, the control plane and the data plane cannot operate.
   - Accessing the controllers using HTTPS or SSH protocols.
2. For the security group, use the option to add inbound security rules. Using the rules, allow all the controller virtual machine IP addresses, to enable the required connectivity between the Cisco SD-WAN Controllers.

   When creating a new inbound security rule, ensure that you complete the following actions:
   - Specify IP ranges, protocol, and so on.
   - For the action of the rule, choose the option to allow the traffic.
3. To verify the connectivity, log in to the virtual machine using the NIC 0 public IP of Cisco SD-WAN Manager.

Verify the Deployment of Cisco SD-WAN Controllers in AWS

- Infrastructure: To verify the deployment of Cisco SD-WAN Controllers within virtual machines in AWS, use the AWS portal to check if the virtual machines hosting each controller are active.
- Services: To verify that Cisco Catalyst SD-WAN services are operating after deployment of the controllers, use the following steps:

1. Check for a successful ping to the virtual machine that hosts Cisco SD-WAN Manager.
2. Log in to the controller instance using AWS console with user as admin. You may be prompted to configure a new password. Once configured, verify login via SSH to the public IP of the controller.
3. Use SSH to connect to Cisco SD-WAN Manager, and use the **request nms all status** command. The output shows the status of all the Cisco SD-WAN Manager services. Confirm that the application server is active.

   The following excerpt of the **request nms all status** command output shows that the application server is active:

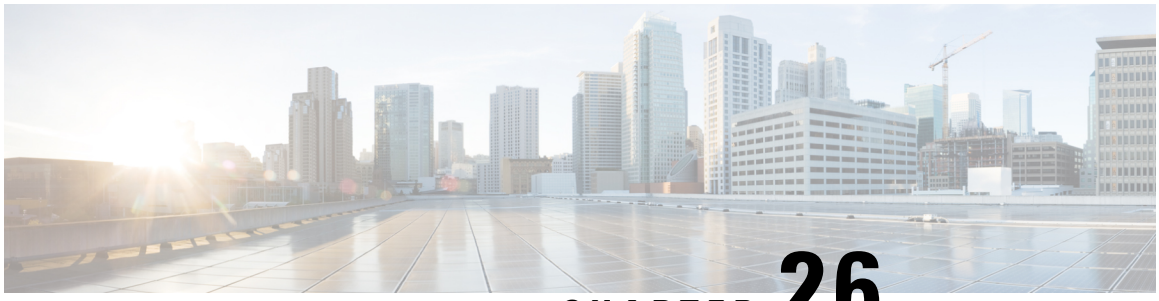
```
vmanage# request nms all status
NMS service proxy
        Enabled: true
        Status: running PID:2881 for 9479s
NMS service proxy rate limit
        Enabled: true
        Status: running PID:4359 for 9521s
NMS application server
        Enabled: true
        Status:  running PID:6131 for 9419s
...
```

4. After installing the controllers, follow the steps in Cisco SD-WAN Overlay Network Bring-Up Process to establish the control connections for the controllers and to verify that each controller is operational.

Monitor the Deployment of Cisco Catalyst SD-WAN Controller in AWS

To monitor the infrastructure status, such as CPU usage and disk usage, use the monitoring tools in the AWS portal.

For information about monitoring the status of Cisco Catalyst SD-WAN services, see the Cisco Catalyst SD-WAN Monitor and Maintain guide.



CHAPTER 26

Troubleshoot Cisco Catalyst SD-WAN Solution

- Overview, on page 427
- Support Articles, on page 427
- Feedback Request, on page 429
- Disclaimer and Caution, on page 429

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
Activate Debugs in vManage	This video provides the steps to activate debugs in Cisco Catalyst SD-WAN Manager
Cisco Catalyst SD-WAN Control Traffic Overhead User Guide	This document describes how to calculate control traffic overhead on an SD-WAN overlay deployment.
Collect an Admin-Tech in SDWAN Environment and Upload to TAC Case	This document describes how to initiate an `admin-tech` in a Cisco Catalyst SD-WAN environment.

Document	Description
Configure Basic Parameters to Form Control Connections on cEdge	This document describes the basic configuration and correct commit order to onboard a cEdge to a Software-Defined Wide Area Network (SD-WAN) overlay.
Configure HSECK9 License on cEdge SD-WAN XE	This document describes how to install and troubleshoot HSECK9 licenses on SD-WAN XE cEdges.
Configure SD-AVC on Cisco Catalyst SD-WAN	This document describes how to configure Software Defined-Application Visibility and Control (SD-AVC) on a Software-Defined Wide Area Network (SD-WAN).
Deploy a CSR1000v/C8000v on Google Cloud Platform	This document describes the procedure to deploy and configure a Cisco Cloud Services Router 1000v (CSR1000v) and Catalyst 8000v (C800v) Edge Router on Google Cloud Platform (GCP).
How To Generate Self-Signed Web Certificate For Cisco Catalyst SD-WAN Manager	This document describes how to generate and install a self-signed web certificate when the existing one is expired on an on-prem Cisco SD-WAN Manager. Cisco does not sign web certificates for such deployments, customers have to sign it by own Certificate Authority (CA) or some third-party CA.
HSEC License FAQs for Cisco Catalyst SD-WAN	This document describes a few queries about the HSEC license for the autonomous and SD-WAN modes.
Manual Certificate Renewal on SD-WAN Controller	This video provides the steps to get controllers certificates renewal.
Modifying "Statistics Configuration > Collection Interval" in a vManage Cluster	This document describes the process of modifying the **Statistics Configuration** > **Collection Interval** in a vManage cluster.
Quick Start Guide - Data Collection for Various Cisco Catalyst SD-WAN Issues	This document describes several SD-WAN issues along relevant data that must be collected in advance before you open a TAC case to improve the speed of troubleshooting and/or problem resolution. This document is broken up into two main technical sections: Cisco SD-WAN Manager and Edge routers. Relevant outputs and command syntax are provided dependent upon the device in question.
Replace a cEdge RMA Router	This document describes how to replace a failed cEdge unit with another one. This consists of a copy of the configuration from the failed router to the replacement router, the removal of this cEdge, and the addition of the new router into the network. This process is similar to vEdge replacement however, the copy option is missed in Cisco SD-WAN Manager for cEdges.

Document	Description
Transfer Files between a cEdge and Cisco Catalyst SD-WAN Manager	This document describes how to transfer files between a remote cEdge and a local Cisco SD-WAN Manager through CLI.
Transfer Files between a vEdge and Cisco Catalyst SD-WAN Manager	This document describes how to transfer files between a remote vEdge and a local Cisco SD-WAN Manager through CLI.
Troubleshoot software image expansion failure due to lack of bootflash space	This document describes how to verify that a device successfully expanded a software image file when changing from Autonomous mode to Controller mode. It indicates how to troubleshoot if the expansion was not successful.
Understand the Web Certificate For Cisco Catalyst SD-WAN Manager	This document describes the difference between the Web Certificate and the Controller Certificates on the Cisco Catalyst SD-WAN solution. This document also explains in detail the Web Certificate and clarifies the use between these two types of certificates.
Upgrade Cisco Catalyst SD-WAN cEdge Router with the Use of CLI or Cisco Catalyst SD-WAN Manager	This document describes the process to upgrade or downgrade an SD-WAN cEdge (Cisco Edge) router in Controller mode from the Command Line (CLI) and from Cisco SD-WAN Manager.
Verify APIs Used by vManage to Gather Statistics	This document describes how to get a specific API call used by Cisco Catalyst SD-WAN Manager to gather statistics from the overlay.

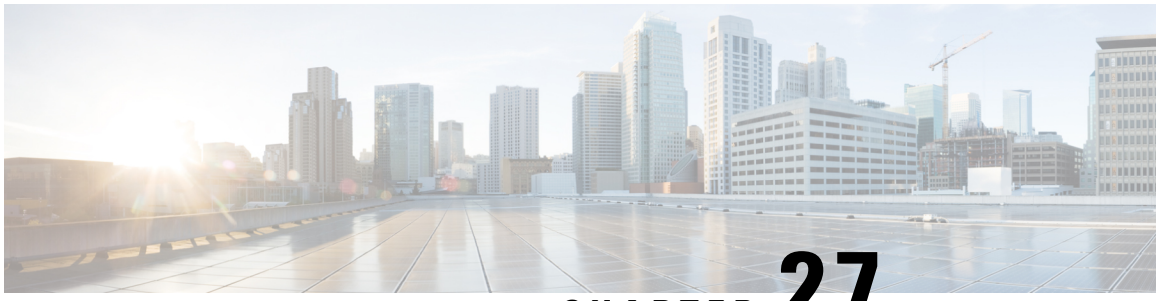
Feedback Request

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.



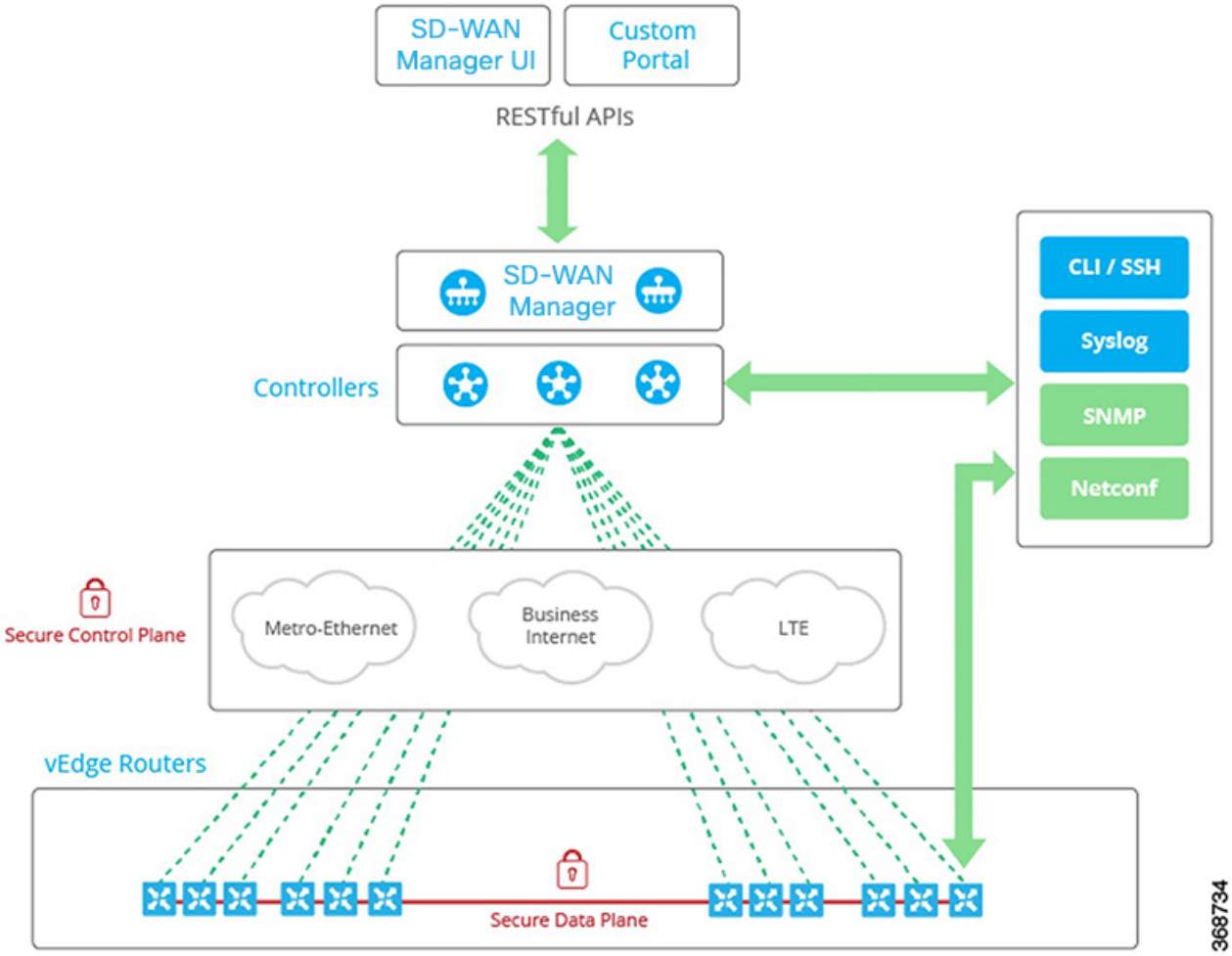
CHAPTER 27

Appendix: Cisco Catalyst SD-WAN Manager How-Tos

- RESTful API for Cisco Catalyst SD-WAN Manager, on page 431
- Replace a vEdge Router, on page 433
- Replace a Cisco IOS XE Catalyst SD-WAN Device, on page 435
- Using Cisco Catalyst SD-WAN Manager on Different Servers, on page 438
- Log In to the Cisco Catalyst SD-WAN Manager Web Application Server, on page 439

RESTful API for Cisco Catalyst SD-WAN Manager

The Cisco SD-WAN Manager supports RESTful (Representational State Transfer) API, which provides calls for retrieving real-time and static information about the Cisco Catalyst SD-WAN overlay network and the devices in the network and for uploading device configuration templates and other configuration-related information. Using the RESTful API, you can design a custom portal for interacting with Cisco SD-WAN Manager.



The Cisco SD-WAN Manager API documentation is provided as part of the Cisco SD-WAN Manager software, at the URL https://*vmanage-ip-address*/apidocs. (More accurately, the full URL includes the Cisco SD-WAN Manager port number, https://*vmanage-ip-address*:8443/apidocs.) *vmanage-ip-address* is the IP address of the Cisco SD-WAN Manager server.

API calls are provided for the following categories of operations:

- Certificate Management
- Configuration
- Device and Device Inventory
- Monitoring
- Real-Time Monitoring
- Troubleshooting Tools

NAT configuration using REST APIs is not supported.

Note Starting from Cisco SD-WAN Release 20.6.1, Cisco SD-WAN Manager supports below API limits:

- API Rate-limit: 100/second
- Bulk API Rate-limit: 48/minute

Real-time monitoring of APIs is CPU intensive and should be used for troubleshooting purposes only. They should not be used continuously for active monitoring of the devices.

For each group of API calls, click **Show/Hide** to list the individual calls and the URL for each call. Each call shows its response class, required parameters, and response messages (status codes).

Click **Try It Out**, to display the request URL for each API call and the format of the response body. The request URL consists of the Cisco SD-WAN Manager's URL, followed by /dataservice. For example, https://10.0.1.32:8443/dataservice/device/interface/statistics/ge0/0?deviceId=172.16.255.11

Below are a few examples of the URLs to use for API calls:

Table 93:

Requested Information	API Call
List all network devices	dataservice/device
Health status of hardware device components, such as CPU, memory, fan, and power	dataservice/device/hardware/environment?deviceId=*system-ip-address*
Status of a device's transport interfaces	dataservice/device/interface?deviceId=*system-ip-address*&port-type=transport
Interface statistics, errors, and packet drops	dataservice/device/interface?deviceId=*system-ip-address*
DTLS/TLS control connection status	dataservice/device/control/connections?deviceId=*system-ip-address*
OMP peering	dataservice/device/omp/peers?deviceId=*system-ip-address*
BGP peering on the service side	dataservice/device/bgp/neighbors?deviceId=*system-ip-address*

Replace a vEdge Router

This section describes how to replace a vEdge router at a particular location. You might do this when a vEdge router has failed completely or when a component in a router, such as one of the power supplies, has failed, and you want to replace the entire router.

At a high level, to replace one vEdge router with another, you simply copy the configuration from the router you are removing to the new router and then put the new router into the network.

Before you can replace the vEdge router in Cisco SD-WAN Manager, Cisco SD-WAN Manager must have learned the chassis number and serial number of the replacement vEdge router.

- If the replacement vEdge router is a router that you have previously received, such as a router that part of your spares inventory, Cisco SD-WAN Manager will have already learned the router's chassis and serial number when you previously uploaded the serial number file to Cisco SD-WAN Manager.
- If you initiated an RMA process and have received a new router as a replacement, you need to upload the updated version of the authorized vEdge serial number file to Cisco SD-WAN Manager.

To replace a failed router using Cisco SD-WAN Manager, perform the following steps:

1. Copy the configuration from the failed router to the replacement router.
2. Invalidate the failed router. Invalidating a router deactivates its certificate and thus removes it from the overlay network.
3. Validate the replacement router, to activate its certificate.

The new router is a complete replacement for the failed router, its configuration is identical to that of the failed router. (Remember, though, that each router has a unique chassis number and a unique serial number in its certificate.) After you copy the configuration from the failed router to the replacement, both routers have the same configurations, including the same IP address. Two routers with the same IP address cannot be present in the network at the same time, one router must be in valid state on Cisco SD-WAN Manager and the other must be in invalid state—or both routers must be in invalid state.

Before You Begin

Ensure that you have uploaded the authorized serial number file to Cisco SD-WAN Manager.

Copy the Configuration from the Failed to the Replacement Router

From Cisco SD-WAN Manager, you copy the configuration from the failed vEdge router to the replacement router.

The vEdge router that you are copying the configuration from can be a device that is active in the overlay network (that is, it is in a valid state) or it can be one that is inactive (that is, it is in invalid state). For example, if you are replacing a router in which one of the two power supplies has failed, the router might still be active in the network, but if you are replacing one that has failed completely, you might have already marked it as invalid to remove it from the network.

The vEdge router that you are copying the configuration to must be in invalid state.

To view the state of a vEdge router or to change the validity state, see Validate or Invalidate a vEdge Router.

To copy the configuration from the failed router to the replacement router:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. For the failed router, click **...** and choose **Copy Configuration**.
3. In the **Copy Configuration** window, choose the replacement router.
4. Click **Update**.

Remove the Failed Router

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. For the failed router, in the **Validate** column, click **Invalid**.
3. Click **OK** to confirm invalidation of the device.
4. Click **Send to Controllers**.

Add the Replacement Router

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. For the replacement router, in the **Validate** column, click **Valid**.
3. Click **OK** to confirm validation of the device.
4. Click **Send to Controllers**.

If you attempt to validate a router that has the same IP address as another router in the network, an error message is displayed, and the validation process is terminated.

Release Information

Introduced in Cisco SD-WAN Manager in Release 15.4.

Replace a Cisco IOS XE Catalyst SD-WAN Device

You might replace a Cisco IOS XE Catalyst SD-WAN device if the device has failed completely or when a component of the device, such as one of the power supplies, has failed.

In general terms, to replace one Cisco IOS XE Catalyst SD-WAN device with another, copy the configuration from the device that you are removing to the new device and then add the new device into the network.

A. Copy the configuration from the device that you are replacing

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. In the list of devices, locate the device to be replaced. In the row of the device, click **…** and choose **Running Configuration**.



Note If Cisco SD-WAN Manager cannot reach the device, skip to step 4 for instructions on logging in to the device directly to copy the configuration information.

3. Copy the text of the configuration and paste it into a text editor.

   The configuration information is useful especially if you choose the manual deployment method for onboarding the new replacement device.

4. If the device is not reachable by Cisco SD-WAN Manager, log in to the device directly and use the following commands on the device to display the configuration information. Copy the configuration information from the output.
   - Display the running configuration and save the output to a text file.

     ```
     show running-config | redirect bootflash:sdwan/ios.cli
     ```

   - Display the SD-WAN running configuration and save the output to a text file.

     ```
     show sdwan running-config | redirect bootflash:sdwan/sdwan.cli
     ```

B. Remove the device from the overlay network

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. In the list of devices, locate the device to be replaced. In the row of the device, in the **Validate** column, click **Invalid**, then **OK**.

Note This step causes any control connections to the device to be lost.

3. Click **Send to Controllers**.
4. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
5. In the list of devices, locate the device to be replaced. In the row of the device, click **…** and choose **Delete WAN Edge**.

C. Add the replacement device to the Cisco SD-WAN Manager inventory

1. Obtain the chassis number and serial number of the replacement device.

Note You can use the **show sdwan certificate serial** command on the device to display this information.

2. Add the new device to the inventory using one of the methods described in the Cisco Catalyst SD-WAN Getting Started Guide.

Note The methods for adding a new device to the inventory are relevant to onboarding devices in general. They are not unique to replacing a device.

D. Apply a device template to the new device, using the same device template that was applied to the device that is being replaced

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. In the row for the template that was used for the device being replaced, click **…** and choose **Export CSV**. The CSV file shows the parameters for each device to which the template is attached.

3. Review the exported CSV file.
   - If the new device is identical to the device being replaced, you do not need to update any of the parameters in the CSV file.
   - If the new device is not identical to the device being replaced, then optionally, you can update parameter values in the CSV file to match the new device, as required. For example, if the replacement device uses a different interface numbering, as compared with the device being replaced, you can update the parameter that specifies interface numbering.

4. To attach the template to the replacement device, do the following:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

   c. In the row for the template that was used for the device being replaced, click **…** and choose **Attach Devices**.
   d. In the **Attach Devices** window, move the replacement device to the **Selected Devices** pane and click **Attach**.
   e. Optionally, you can update parameters in the template before applying it to the device, using one of the following methods:
      - In the row of the replacement device, click **…** and choose **Edit Device Template**. Edit any parameters, as needed.
      - Upload the CSV file that you downloaded and edited to update the parameters for the replacement device. To upload the CSV file, click **Upload** (up arrow button) and navigate to the CSV file.

E. Onboard the new device

Use one of the following methods to onboard the new device.

Note The methods for onboarding a new device to the inventory are relevant to onboarding devices in general. They are not unique to replacing a device.

- Plug and Play (PnP)

  For information, see the Plug and Play Onboarding Workflow section of the Cisco Catalyst SD-WAN Getting Started Guide, and see the Cisco Catalyst SD-WAN: WAN Edge Onboarding guide.

- Bootstrap

  For information, see the Non-PnP Onboarding section of the Cisco Catalyst SD-WAN Getting Started Guide, and see the bootstrap deployment section of the Cisco Catalyst SD-WAN: WAN Edge Onboarding guide.

- Manual deployment

Note To configure the new device, you can use the configuration files that you saved earlier in part A.

Note The manual deployment method requires installing a root certificate authority (CA) for the new device.

For information, see the Cisco Catalyst SD-WAN: WAN Edge Onboarding guide.

For information about installing a root CA, see the Enterprise Certificates section of the Cisco Catalyst SD-WAN Getting Started Guide.

Using Cisco Catalyst SD-WAN Manager on Different Servers

. You can perform the following operations in parallel from one or more Cisco SD-WAN Manager servers:

- From the Cisco SD-WAN Manager menu, select **Maintenance** > **Software Upgrade** to do the following:
  - Upgrade the software image on a device.
  - Activate a software image on a device.
  - Delete a software image from a device.
  - Set a software image to be the default image on a device.
- From the Cisco SD-WAN Manager menu, select **Maintenance** > **Device Reboot** to reboot a device.
- From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates** to manage templates:
  - Attach devices to a device template.
  - Detach devices from a device template.
  - Change the variable values for a device template that has devices attached to it.

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. When you click **Update** > **Configure Devices**, all other template operations—including attach devices, detach devices, and edit device values—are locked on all Cisco SD-WAN Manager servers until the update operation completes. This means that a user on another Cisco SD-WAN Manager server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more Cisco SD-WAN Manager servers, at the same time. However, if any one of these operations is in progress on one Cisco SD-WAN Manager server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Log In to the Cisco Catalyst SD-WAN Manager Web Application Server

The Cisco SD-WAN Manager runs as a web application server through which you log in to a running Cisco SD-WAN Manager.

In an overlay network with a single Cisco SD-WAN Manager, to log in to the server, use HTTPS, and specify the IP address of the server. Enter a URL in the format https://*ip-address*:8443, where 8443 is the port number used by Cisco SD-WAN Manager. On the login page, enter a valid username and password, and then click **Log In**. You have five chances to enter the correct password. After the fifth incorrect attempt, you are locked out of the device, and you must wait for 15 minutes before attempting to log in again.

In an overlay network that has a cluster of Cisco SD-WAN Managers, the cluster allows you to log in to one of the Cisco SD-WAN Managers that is operating in the role of a web application server. Use HTTPS, specifying the IP address of one of the Cisco SD-WAN Managers, in the format https://*ip-address*:8443. The cluster software load-balances login sessions among the individual Cisco SD-WAN Managers that are acting as web application servers. You cannot control which of the individual Cisco SD-WAN Managers you log in to.

With a Cisco SD-WAN Manager cluster, if you enter invalid login credentials, it might take some time for you to see an invalid login error message, and the amount of time increases as the size of the cluster increases. This delay happens because each Cisco SD-WAN Manager attempts sequentially to validate the credentials. If none of the Cisco SD-WAN Manager servers validate you, only then do you see an invalid login error message.

To determine which Cisco SD-WAN Manager you are logged in to, look in the Cisco SD-WAN Manager toolbar, which is located at the top of the screen. To view more information about this particular Cisco SD-WAN Manager server, enter the name of the server in the Search filter of the **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: To determine which Cisco SD-WAN Manager you are logged in to, look in the Cisco SD-WAN Manager toolbar, which is located at the top of the screen. To view more information about this particular Cisco SD-WAN Manager server, enter the name of the server in the Search filter of the **Monitor** > **Network**.