Cisco Catalyst SD-WAN Onboarding Guide, Releases 26.x and Later

Cisco SD-WAN
Updated July 7, 2026

Topics included

1 Automated Bring-Up Sequence....9

Automated Bring-Up Sequence....10
ZTP automatic authentication process....10
Authentication between Cisco SD-WAN Controller and Cisco SD-WAN Validator....10
Authentication Between Cisco SD-WAN Controllers....11
Authentication between Cisco SD-WAN Validator and a WAN edge device....12
Authentication between the WAN edge device and Cisco SD-WAN Manager....13
Authentication between Cisco SD-WAN Controller and a WAN edge device....15

2 Onboarding Devices Using a Bootstrap File....17

Feature history for bootstrap file onboarding....18
One Touch Provisioning to onboard Cisco IOS XE Catalyst SD-WAN Devices using generic bootstrap configuration....18
Generic bootstrap configurations process....19
Onboard a Cisco IOS XE Catalyst SD-WAN Device using generic bootstrap configuration....19
Remove a Cisco IOS XE Catalyst SD-WAN Device onboarded using generic bootstrap configuration....21
On-Site bootstrap process for Cisco IOS XE Catalyst SD-WAN devices....21
Restrictions for on-site bootstrap process....22
Perform the on-site bootstrap process for Cisco Catalyst SD-WAN devices....22

3 Firewall Ports for Cisco Catalyst SD-WAN Deployments....25

Cisco Catalyst SD-WAN-specific port terminology....26
Port offset....26
Port hopping....26
Effects of port hopping....29
Ports used by Cisco vEdge Devices....29
Ports used by Cisco Catalyst SD-WAN devices running multiple vCPUs....31
Administrative ports used by Cisco SD-WAN Manager....31
Configure the port offset....33
Perform port hopping manually....34

4 Onboarding Cisco SD-WAN Manager....35

Cisco SD-WAN Manager personas....36
Storage devices....37
Software download process....37
Feature history for device software installation....38
Platform support....39
Cisco IOS XE image compatibility....40

Self-signed trustpoint....40
Autonomous and controller modes....40
Restrictions for installing and upgrading device software....41
Software Installation for Cisco IOS XE Routers....42
Software image type....42
Installing software on select platforms....43
Install software on the Cisco Catalyst 8000V Edge Software platform....43
Install software on the Cisco CSR 1000v platform....44
Plug and Play onboarding....44
Plug and Play onboarding workflow....44
Mode discovery with Plug and Play onboarding....45
Automatic IP address detection....45
Non-Plug and Play onboarding....46
New installation: Mode change device day zero scenario....46
Change a device to Autonomous mode....47
Change a device to Controller mode....47
Viewing the sdwaninstaller directory....48
Mode discovery and mode change with a bootstrap file....48
Reset a device to a Controller mode day zero configuration using CLI commands....50
Configuration persistence during mode switch....50
Verifying Controller and Autonomous modes....51
Change the console port access after installation, in Controller mode....53
Restoring Smart Licensing after switching modes....54
Restore Smart License reservation....54
Restore Smart Licensing....55
Deploy a Cisco SD-WAN instance....55
Create a Cisco SD-WAN manager VM instance on VMware ESXi....56
Launch vSphere Client and Create Cisco Catalyst SD-WAN Manager VM Instance 56
Create a new virtual disk....56
Add additional vnics....57
Connect a VM instance to the Cisco SD-WAN manager console....57
Cisco SD-WAN Manager VM Instance on KVM....58
Create a VM instance for Cisco SD-WAN Manager on the KVM hypervisor....58
Connect to a Cisco SD-WAN manager instance....60
Configure Cisco SD-WAN manager....60

5 Onboarding Cisco SD-WAN Validator....65

Deploy Cisco Catalyst SD-WAN Validator....66
Create Cisco Catalyst SD-WAN Validator VM instance on ESXi....66
Launch vSphere Client and create a Cisco Catalyst SD-WAN Validator VM instance....67
Add a vNIC for the tunnel interface....67
Start the Cisco Catalyst SD-WAN Validator VM instance and connect to the console....68
Create Cisco SD-WAN Validator VM instance on KVM....68
Configure the vBond orchestrator....69

Add Cisco SD-WAN Validator to the overlay network....73
Start the enterprise ZTP server....74
Requirements for ZTP....74
Configure a Router to be a ZTP Server....76

6 Onboarding Cisco SD-WAN Controller....79
Deploy a Cisco Catalyst SD-WAN Controller controller....80
Create Cisco Catalyst SD-WAN Controller VM instance on ESXi....80
Launch vSphere Client and create a Cisco Catalyst SD-WAN Controller VM instance....81
Add a vNIC for the management interface....81
Start the Cisco Catalyst SD-WAN Controller VM instance and connect to the console....82
Create a Cisco SD-WAN Controller VM instance on KVM....82
Configure the Cisco Catalyst SD-WAN Controller....83
Add Cisco SD-WAN Controller to the overlay network....87

7 Add SD-WAN controller and SD-WAN validator components....89
Feature history for SD-WAN controller and SD-WAN validator components workflow....90
Control components certificate management workflow....90
Supported solutions for the add SD-WAN controller and SD-WAN validator workflow....90
Supported environments for the add SD-WAN controller and SD-WAN validator components workflow....90
Requirements for adding SD-WAN controller and SD-WAN validator components....90
Add SD-WAN controllers or SD-WAN validators using a workflow....91

8 First Time Settings for SD-WAN Manager....93
Feature history for first time settings....94
First time settings for SD-WAN Manager....94
Enable multitenancy on SD-WAN Manager 96
Configure the organization name....96
Configure common SD-WAN Control Component network settings....96
Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier....106
Configure cloud services....106
Configure certificate settings....107
Add Cisco SD-WAN Controller and Cisco SD-WAN Validator....112
Configure SD-WAN Validator IP address....112
Configure identity provider settings....112
Configure users and access....113
Alarm notification settings....114
Configure account lockout settings....114
Configure a web server certificate for Cisco SD-WAN Manager....115

9 Quick Connect Workflow....117
Feature history for the Quick Connect workflow....118
Quick Connect workflow for SD-WAN Manager....118

Prerequisites for using the Quick Connect Workflow....119
Restrictions for the Quick Connect Workflow....119
Run the Quick Connect Workflow....120
Auto Sync for uploading devices....121
Auto Sync with Cisco PnP, SD-WAN Manager 20.18.1 and earlier....121
Auto Sync with ZTP....122
Upload devices for onboarding with Auto Sync....122
Upload devices manually to SD-WAN Manager....123
Upload devices to SD-WAN Manager manually....123
Quick Connect behavior with manual upload of devices....123

10 Installing Cisco SD-WAN Control Components in the AWS Cloud....125
Feature history for installing Cisco SD-WAN Control Components in the AWS Cloud....126
Installing Cisco SD-WAN Control Components in AWS....126
Prerequisites for SD-WAN Control Components deployment in AWS....127
Use cases for SD-WAN Control Component deployment in AWS....128
Installing Cisco SD-WAN Control Components in AWS....128
Install SD-WAN Control Components in AWS....129
Request AWS AMI images....130
Create a virtual network, subnets, and network security group in AWS....130
Create a virtual machine for the SD-WAN Control Components....131
Configure the Security Group....133
Verify the deployment of SD-WAN Control Component s in AWS....133
Monitor the deployment of SD-WAN Control Component in AWS....134

11 Deploying SD-WAN Control Components in Microsoft Azure....135
Deploy SD-WAN Control Components in Microsoft Azure....136
Scenarios for SD-WAN Control Component deployments in Azure....137
Deploy an SD-WAN Control Component image in Azure....137
Create an SD-WAN Control Component image in Azure....137
Create a Virtual Network, Subnets, and Network Security Group in Azure....139
Create a virtual machine for the SD-WAN Control Component....140
Configure the Network Security Group....142
Verify the deployment of SD-WAN Control Components in Azure....143
Monitor the deployment of SD-WAN Control Components in Azure....144

12 Device Software Installation, Cisco IOS XE 17.2.1r and Later....145
Feature history for device software installation....146
Platform support....146
Cisco IOS XE image compatibility....147
Self-signed trustpoint....147
Autonomous and controller modes....148
Restrictions for installing and upgrading device software....148

Software Installation for Cisco IOS XE Routers....150
Software image type....150
Installing software on select platforms....150
Install software on the Cisco Catalyst 8000V Edge Software platform....150
Install software on the Cisco CSR 1000v platform....151
Plug and Play onboarding....151
Plug and Play onboarding workflow....151
Mode discovery with Plug and Play onboarding....152
Automatic IP address detection....153
Non-Plug and Play onboarding....154
New installation: Mode change device day zero scenario....154
Change a device to Autonomous mode....154
Change a device to Controller mode....155
Viewing the sdwaninstaller directory....155
Mode discovery and mode change with a bootstrap file....156
Reset a device to a Controller mode day zero configuration using CLI commands....157
Configuration persistence during mode switch....158
Verifying Controller and Autonomous modes....158
Change the console port access after installation, in Controller mode....160
Restoring Smart Licensing after switching modes....161
Restore Smart License reservation....161
Restore Smart Licensing....162

13 Cisco SD-AVC....163
Feature history for Cisco SD-AVC....164
Cisco SD-AVC....164
Cloud-hosted SD-AVC....164
Restrictions for cloud-hosted SD-AVC....165
Installing and enabling Cisco SD-AVC, Releases 20.3.1 and later....166
Enable Cisco SD-AVC on Cisco vManage Release 20.3.1 through SD-WAN Manager 20.16.x....166
Enable Cisco SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices....167

14 SD-AVC Cloud Connector....169
Feature history for Cisco SD-AVC Cloud Connector....170
Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later....170
Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x....171
Enable Cloud Services....177

15 Cisco Services Authentication....179
Feature history of Cisco services registration....180
Authentication for Cisco services....180
Restrictions for authenticating Cisco services....180
Authenticate Cisco services....180

1 Automated Bring-Up Sequence

Topics:

- Automated Bring-Up Sequence
- ZTP automatic authentication process
- Authentication between Cisco SD-WAN Controller and Cisco SD-WAN Validator
- Authentication Between Cisco SD-WAN Controllers
- Authentication between Cisco SD-WAN Validator and a WAN edge device
- Authentication between the WAN edge device and Cisco SD-WAN Manager
- Authentication between Cisco SD-WAN Controller and a WAN edge device

Introduces the automated bring-up sequence, outlining the steps and processes required to initialize and configure devices.

Automated Bring-Up Sequence

Details the sequence and workflow of automated bring-up, including key stages, prerequisites, and mechanisms that facilitate efficient and reliable SD-WAN system onboarding.

After WAN edge devices boot and run their initial configurations, the Cisco SD-WAN Validator automatically leads the second part of the bring-up process. The WAN edge devices establish encrypted communication channels among themselves under Cisco SD-WAN Validator. They automatically validate and authenticate each other over these channels, forming an operational overlay network. Once the overlay network is active, the WAN edge devices automatically receive and activate their full configurations from the Cisco SD-WAN Manager server. (You must manually configure each Cisco SD-WAN Manager server.) After the initial configurations, Cisco SD-WAN Validator initiates the automatic bring-up sequence.

ZTP automatic authentication process

Explains the ZTP automatic authentication process, outlining device onboarding, cryptographic exchanges, and certificate validation essential for secure connectivity in SD-WAN environments.

Automatic validation and authentication of WAN edge devices during bring-up require that Cisco SD-WAN Validator and Cisco SD-WAN Controller know the serial and chassis numbers of authorized devices.

- **Serial number**: Each WAN edge device has a 40-byte serial number included in its certificate. For Cisco SD-WAN Validator and Cisco SD-WAN Controller, certificates are an enterprise root CA. For WAN edge routers, the certificate resides in the hardware's trusted board ID chip.
- **Chassis number**: Only WAN edge routers have chassis numbers, with a one-to-one mapping to their serial numbers.

Cisco SD-WAN Validator and Cisco SD-WAN Controller learn these numbers during initial device configuration:

- **Controller authorized serial numbers**: Cisco SD-WAN Manager learns serial numbers for authorized controllers when creating a CSR and installing the signed certificate. You download these serial numbers to Cisco SD-WAN Validator, which pushes them to Cisco SD-WAN Controller during automatic authentication.
- **WAN edge authorized serial number file**: This file contains serial and chassis numbers of authorized WAN edge routers. You upload it to Cisco SD-WAN Validators and Cisco SD-WAN Controllers.

All devices must share the same organization name, configured on Cisco SD-WAN Manager and included in device configuration files and certificates. This name is case-sensitive.

Authentication between Cisco SD-WAN Controller and Cisco SD-WAN Validator

Describes authentication procedures between key SD-WAN infrastructure components, emphasizing secure credential exchanges, verification steps, and trust establishment during automated bring-up.

Cisco SD-WAN Controller initiates the first authentication with Cisco SD-WAN Validator, the first two devices on the Cisco Catalyst SD-WAN overlay network to validate and authenticate each other. When the Controller boots, it connects to the Validator, allowing the Validator to learn about the Controller. Both devices then automatically start a two-way authentication process over an encrypted DTLS channel secured by RSA keys generated at boot. The authentication handshakes occur in parallel, but for clarity, they are often illustrated sequentially.

If authentication succeeds, the devices establish a permanent DTLS communication channel. If any authentication step fails, the device detecting the failure tears down the connection, terminating the attempt.

The Controller knows how to reach the Validator because its configuration includes the Validator's IP address or DNS name. The Validator is ready to respond because:

- Its role as the authentication system is configured.

- It has received the Controller authorized serial numbers downloaded from Cisco SD-WAN Manager.

If the Validator is not yet started when the Controller initiates authentication, the Controller periodically retries until successful.

The detailed authentication steps are:

1. The Controller initiates an encrypted DTLS connection to the Validator.
2. The Validator sends its trusted root CA signed certificate and the WAN edge authorized serial number file to the Controller.
3. The Controller extracts the organization name from the Validator's certificate and compares it to its configured organization name. If they match, the Controller confirms the Validator's organization; if not, it tears down the connection.
4. The Controller verifies the Validator's certificate signature using the root CA chain (Symantec or enterprise CA). If valid, it accepts the certificate; otherwise, it tears down the connection.
5. The Controller sends its trusted root CA signed certificate to the Validator.
6. The Validator extracts the Controller's serial number from the certificate and checks it against its authorized serial number file. If no match exists, it tears down the connection.
7. The Validator compares the organization name from the Controller's certificate to its configured name. If they match, it confirms the Controller's organization; if not, it tears down the connection.
8. The Validator verifies the Controller's certificate signature using the root CA chain. If valid, it accepts the certificate; otherwise, it tears down the connection.

After these checks, the bidirectional authentication completes, and the DTLS connection transitions from temporary to permanent. The devices establish an OMP session over this connection.

In networks with multiple Controllers for redundancy, this authentication process repeats between each Controller and the Validator. Controllers learn about each other's IP addresses from the Validator and synchronize route information. For higher availability, connect Controllers to the WAN network through different NAT devices.

Each Validator maintains permanent DTLS connections equal to the number of Controllers in the network topology. These connections form the control plane; no data traffic flows over them. After all Controllers register with the Validator, the Validator and Controllers are ready to validate and authenticate WAN edge routers in the Cisco Catalyst SD-WAN network.

Authentication Between Cisco SD-WAN Controllers

Outlines the authentication processes between Cisco Catalyst SD-WAN Controllers, detailing mutual verification methods and secure communication protocols used during system initialization.

In a domain with multiple SD-WAN Controller, the controllers authenticate each other to establish a full mesh of permanent DTLS connections for synchronizing OMP routes. Each SD-WAN Controller learns the IP addresses of other controllers from the SD-WAN Validator.

During the authentication handshake with the SD-WAN Validator, each controller receives a copy of the authorized serial number file for SD-WAN Controllers. If this file contains more than one serial number, it indicates the network may have multiple controllers.

When a SD-WAN Controller authenticates with the SD-WAN Validator, the validator sends it the IP addresses of other authenticated controllers. If the validator later discovers another controller, it sends that controller's address to the already authenticated controllers.

The controllers then authenticate each other by performing the following steps sequentially (though authentication occurs in parallel):

1. Controller1 initiates an encrypted DTLS connection to controller2 and sends its trusted root CA signed certificate.

2. Controller2 extracts controller1's serial number from the certificate using its chain of trust and verifies it matches one in the authorized serial number file. If no match exists, controller2 tears down the DTLS connection.
3. Controller2 extracts the organization name from the certificate and compares it to its locally configured organization name. If they match, controller2 confirms controller1's organization; otherwise, it tears down the connection.
4. Controller2 verifies the certificate's signature using the root CA chain (Symantec or enterprise CA). If valid, controller2 accepts the certificate; if invalid, it tears down the connection.

After these checks, controller2 completes authentication of controller1.

Controller1 then authenticates controller2 by performing the same steps:

1. Controller2 sends its trusted root CA signed certificate to controller1.
2. Controller1 verifies controller2's serial number against the authorized serial number file, tearing down the connection if no match exists.
3. Controller1 compares the organization name from the certificate to its local configuration, tearing down the connection if they do not match.
4. Controller1 verifies the certificate's signature using the root CA chain, tearing down the connection if invalid.

After these checks, controller1 completes authentication of controller2, and the temporary DTLS connection becomes permanent.

Once all SD-WAN Controllers have registered with the SD-WAN Validatorr, the validator and controllers are ready to validate and authenticate the WAN Edge routers in the Cisco Catalyst SD-WAN network.

Authentication between Cisco SD-WAN Validator and a WAN edge device

Details authentication between validator and WAN edge devices, highlighting credential validation, certificate exchanges, and trusted onboarding for secure SD-WAN connectivity.

When you deploy a WAN edge device, it must first:

- Establish a secure connection with Cisco SD-WAN Manager to receive its full configuration.
- Establish a secure connection with Cisco SD-WAN Controller to participate in the Cisco Catalyst SD-WAN overlay network.

The WAN edge device automatically discovers Cisco SD-WAN Manager and Cisco SD-WAN Controller with help from Cisco SD-WAN Validator. The WAN edge device's initial configuration includes the Cisco SD-WAN Validator's IP address or DNS name. Using this, the WAN edge device establishes a DTLS connection with Cisco SD-WAN Validator. Both devices authenticate each other automatically in a two-way process to confirm they are valid WAN edge devices. Upon successful authentication, Cisco SD-WAN Validator sends the WAN edge device the IP addresses of Cisco SD-WAN Manager and Cisco SD-WAN Controller. The WAN edge device then tears down its connection with Cisco SD-WAN Validator and begins establishing secure DTLS connections with the other two devices.

After booting and performing initial configuration, WAN edge devices automatically seek their Cisco SD-WAN Validator. Cisco SD-WAN Validator and Cisco SD-WAN Controllers recognize and authenticate WAN edge devices because the authorized device list file is installed on both.

The WAN edge device uses the configured IP address or DNS name of Cisco SD-WAN Validator to reach it. Cisco SD-WAN Validator is ready to respond because:

- Its role as the authentication system is defined in its initial configuration.
- The authorized serial number file for WAN edge devices is installed on Cisco SD-WAN Validator.

If Cisco SD-WAN Validator is not yet started when the WAN edge device initiates authentication, the device retries periodically until successful.

The following steps describes a detailed authentication process between Cisco SD-WAN Validator and WAN edge device:

1. The WAN edge device initiates an encrypted DTLS connection to Cisco SD-WAN Validator's public IP address. RSA encryption secures this connection. Each device generates an RSA private-public key pair at boot. Cisco SD-WAN Validator uses the outer IP address in the packet to detect if the WAN edge device is behind NAT and maps the public IP and port to the private IP.
2. Over the encrypted DTLS channel, both devices authenticate each other in parallel.

WAN edge device authenticates Cisco SD-WAN Validator:

- Cisco SD-WAN Validator sends its trusted root CA signed certificate.
- The WAN edge device extracts the organization name from the certificate and compares it to its configured organization name. If they match, the validator is considered valid; otherwise, the DTLS connection is torn down.
- The WAN edge device verifies the certificate's signature using the root CA chain (Symantec or enterprise CA). If invalid, it tears down the connection.

Cisco SD-WAN Validator authenticates the WAN edge device:

- Cisco SD-WAN Validator sends a 256-bit random challenge.
- The WAN edge device responds with its serial number, chassis number, board ID certificate, and the signed 256-bit random value using its private key.
- Cisco SD-WAN Validator verifies the serial and chassis numbers against its authorized device list. If no match, it tears down the connection.
- It verifies the signature of the random value using the WAN edge device's public key from the board ID certificate. If invalid, it tears down the connection.
- It validates the board ID certificate using the root CA chain. If invalid, it tears down the connection.

After successful mutual authentication, Cisco SD-WAN Validator sends the following in parallel:

- To the WAN edge device:
  - IP addresses of Cisco SD-WAN Controllers (public or NAT-mapped private and public IPs with ports).
  - Serial numbers of authorized Cisco SD-WAN Controllers.
  - If the WAN edge device is behind NAT, a request to initiate a session with Cisco SD-WAN Controller.
- To Cisco SD-WAN Controller:
  - A message announcing the new WAN edge device.
  - If the WAN edge device is behind NAT, a request to initiate a session with the WAN edge device.

Finally, the WAN edge device tears down the DTLS connection with Cisco SD-WAN Validator.

Authentication between the WAN edge device and Cisco SD-WAN Manager

Explains authentication steps between WAN edge devices and Cisco SD-WAN Manager, covering verification mechanisms and secure onboarding procedures within the automated bring-up sequence.

After the Cisco WAN edge device and SD-WAN Validator authenticate each other, the WAN edge device receives its full configuration over a DTLS connection with SD-WAN Manager:

- The WAN edge device establishes a DTLS connection with SD-WAN Manager.
- SD-WAN Manager sends the configuration file to the WAN edge device.

- Upon receiving the configuration file, the WAN edge device activates its full configuration.
- The WAN edge device starts advertising prefixes to SD-WAN Controller.

If you do not use SD-WAN Manager, you can log in to the WAN edge device and manually load its configuration file or configure the device manually.

The following steps describe the detailed authentication process between a WAN edge device and SD-WAN Manager:

1. The WAN edge device initiates an encrypted DTLS connection to the IP address of SD-WAN Manager. RSA encryption secures this connection. Each device generates an RSA private-public key pair at boot. SD-WAN Manager receives the WAN edge device's original interface address and uses the outer IP address in the received packet to determine if the WAN edge device is behind a NAT. If so, SD-WAN Manager maps the WAN edge device's public IP address and port to its private IP address.
2. Over this encrypted DTLS channel, the WAN edge device and SD-WAN Manager authenticate each other in parallel.

WAN edge device authenticates SD-WAN Manager:

- SD-WAN Manager sends its trusted root CA signed certificate to the WAN edge device.
- The WAN edge device extracts the organization name from the certificate using its chain of trust and compares it to the organization name configured on the device. If they match, the WAN edge device confirms the organization of SD-WAN Manager; otherwise, it tears down the DTLS connection.
- The WAN edge device verifies the certificate's signature using the root CA chain (Symantec or enterprise CA). If the signature is valid, the certificate is considered valid; if not, the DTLS connection is torn down.

After these checks, the WAN edge device completes authentication of SD-WAN Manager.

SD-WAN Manager authenticates the WAN edge device:

- SD-WAN Manager sends a 256-bit random challenge to the WAN edge device.
- The WAN edge device responds with:
  - Its serial number
  - Its chassis number
  - Its board ID certificate (for hardware WAN edge devices) or signed certification (for WAN edge Cloud devices)
  - The 256-bit random value signed by the WAN edge device's private key
- SD-WAN Manager compares the serial and chassis numbers to its authorized device list file. If no match exists, it tears down the DTLS connection.
- It verifies the signature of the 256-bit random value using the WAN edge device's public key extracted from the board ID certificate. If invalid, it tears down the connection.
- It validates the board ID certificate using the root CA chain. If invalid, it tears down the connection.

After these checks, SD-WAN Manager completes authentication of the WAN edge device.

When mutual authentication succeeds, SD-WAN Manager sends the configuration file to the WAN edge device. Upon receiving the configuration, the WAN edge device activates its full configuration and starts advertising prefixes to SD-WAN Controller.

Authentication between Cisco SD-WAN Controller and a WAN edge device

Describes authentication workflows between Cisco SD-WAN Controllers and WAN edge devices, focusing on secure credential exchanges, device validation, and trust establishment within the SD-WAN framework.

The final step in the automatic authentication process involves mutual authentication between the SD-WAN Controller and the WAN edge device. The controller authenticates the WAN edge device to confirm it belongs to the network, and the WAN edge device authenticates the controller. Upon successful authentication, the DTLS connection between the two devices becomes permanent, and the controller establishes an OMP peering session over this connection. The WAN edge device then begins sending data traffic over the Cisco Catalyst SD-WAN overlay network.

To initiate the session, either device starts an encrypted DTLS connection to the other, using RSA encryption. Each device generates an RSA private-public key pair at boot.

SD-WAN Controller authenticates the WAN edge device as follows:

1. The controller sends a 256-bit random challenge to the WAN edge device.
2. The WAN edge device responds with:
   - Its serial number
   - Its chassis number
   - Its board ID certificate
   - The 256-bit random value signed by its private key
3. The controller compares the serial and chassis numbers against its authorized device list. If no match exists, it tears down the DTLS connection.
4. The controller verifies the signature on the random value using the public key extracted from the device's board ID certificate. If invalid, it tears down the connection.
5. The controller validates the board ID certificate using the root CA chain. If invalid, it tears down the connection.
6. The controller compares the response to the original challenge issued by the SD-WAN Validator. If they match, authentication succeeds; otherwise, the connection is torn down.

After these checks, the controller confirms the WAN edge device is valid.

The WAN edge device authenticates the SD-WAN Controller as follows:

1. The controller sends its trusted root CA signed certificate to the WAN edge device.
2. The WAN edge device extracts the controller's serial number from the certificate and verifies it against its authorized serial number list. If no match exists, it tears down the connection.
3. The WAN edge device extracts the organization name from the certificate and compares it to its configured organization name. If they do not match, it tears down the connection.
4. The WAN edge device verifies the certificate's signature using the root CA chain (Symantec or enterprise CA). If invalid, it tears down the connection.

After these checks, the WAN edge device completes authentication of the controller.

The DTLS connection used for authentication becomes permanent, and the two devices establish an OMP session over it to exchange control plane traffic.

This authentication process repeats for every SD-WAN Controller and WAN edge device introduced into the overlay network. Each WAN edge device must connect to at least one controller via a successful DTLS connection. For redundancy, domains typically have multiple controllers, allowing each WAN edge device to connect to more than one controller.

Over the OMP session, the WAN edge device sends control plane information to the controller to help it learn the network topology:

- The WAN edge device advertises service-side prefixes and routes learned from local static and dynamic routing protocols (BGP and OSPF).
- Each WAN edge device has a transport locator (TLOC), the address of the interface connecting to the WAN transport network or NAT gateway. Once the DTLS connection is established, OMP registers the TLOCs with the controller.
- The WAN edge device advertises IP addresses of services on its service-side network, such as firewalls and intrusion detection devices.

The controller installs these OMP routes in its routing database and advertises them to other WAN edge devices in the overlay network. It also updates each WAN edge device with OMP route information learned from other devices. The controller can apply inbound policies on received routes before installing them and outbound policies before advertising routes.

2 Onboarding Devices Using a Bootstrap File

Topics:

- Feature history for bootstrap file onboarding
- One Touch Provisioning to onboard Cisco IOS XE Catalyst SD-WAN Devices using generic bootstrap configuration
- Generic bootstrap configurations process
- Onboard a Cisco IOS XE Catalyst SD-WAN Device using generic bootstrap configuration
- Remove a Cisco IOS XE Catalyst SD-WAN Device onboarded using generic bootstrap configuration
- On-Site bootstrap process for Cisco IOS XE Catalyst SD-WAN devices

Feature history for bootstrap file onboarding

Lists the development milestones and release information for one touch provisioning to onboard using generic bootstrap configuration, including feature description.

This table describes the developments of this feature, by release.

Table 1: 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 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 SD-WAN Manager as an unclaimed WAN edge device. To complete the onboarding, claim the device on SD-WAN Manager and use configuration groups to configure the system IP address and site ID.

One Touch Provisioning to onboard Cisco IOS XE Catalyst SD-WAN Devices using generic bootstrap configuration

Facilitates the onboarding of multiple devices to the network by utilizing a generic bootstrap configuration that omits device-specific details. This process simplifies deployment by allowing devices to connect to the controller before final template assignment.

A generic bootstrap configuration is a provisioning file that enables a Cisco IOS XE Catalyst SD-WAN device to connect to the Cisco SD-WAN Validator without requiring device-specific identifiers like the UUID.

- Includes the organization name and Cisco SD-WAN Validator IP address.
- Contains a Cisco SD-WAN Manager -signed certificate for device authentication.
- Enables a DHCP client on the WAN interface to acquire network connectivity.

Generic Bootstrap Configuration Details

The generic bootstrap configuration provides the essential settings required for a device to establish initial contact with the overlay network. Once the device connects, it appears as an unclaimed WAN edge device on Cisco SD-WAN Manager, where you can complete the onboarding process by attaching a device template.

The configuration includes the following components:

- 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.

Generic bootstrap configurations process

Describes how the generic bootstrap configuration initializes a device and integrates it into the overlay network. This process ensures secure authentication and automated connectivity for WAN edge devices.

The process involves the following key components:

- SD-WAN Manager: Orchestrates device authentication and template management.
- Cisco IOS XE Catalyst SD-WAN device: The WAN edge device being initialized.
- SD-WAN Validator: Facilitates initial device discovery and registration.
- SD-WAN Controller: Manages control connections and overlay network membership.

These stages describe the lifecycle of a generic bootstrap configuration from initial setup to network integration.

1. Initial configuration and device reset.
   - Select the interface serving as the VPN 0 (WAN) interface on the Cisco IOS XE Catalyst SD-WAN device during configuration generation on SD-WAN Manager .
   - Copy the configuration file to the device bootflash and reset the device to initialize the bootstrap settings.
2. Network discovery and authentication.
   - The bootstrap configuration enables a DHCP client on the VPN 0 interface to acquire network details.
   - The device connects to the SD-WAN Validator and appears as an unclaimed WAN edge device.
   - Upon claiming the device on SD-WAN Manager , the system authenticates the device using its installed certificate.
3. Template attachment and network integration.
   - Associate and deploy a configuration group containing the system IP and site ID to the device.
   - The device establishes control connections to SD-WAN Control Components to join the overlay network.

Onboard a Cisco IOS XE Catalyst SD-WAN Device using generic bootstrap configuration

Provisions a Cisco IOS XE Catalyst SD-WAN Device by generating and applying a generic bootstrap configuration file. This process enables the device to connect to the network and register with Cisco SD-WAN Manager .

1. Enable One Touch Provisioning (Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier) .
   a) From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** .
   b) Check if **One Touch Provisioning** is **Enabled** .
   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.**
c) Save the generic bootstrap configuration file.

The file is named in the format `<filename>.cfg`.

d) Rename the generic bootstrap configuration file as `ciscosdwan.cfg`.
e) Copy the `ciscosdwan.cfg` file to a bootable USB drive or to the bootflash of the device.

4. If you are using a USB drive, plug the USB drive into the device.
5. 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.

6. 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.

7. 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** .

8. Associate a configuration group to the device.
   a) Ensure that the template includes the system IP address and the site ID.
   b) Push the template to the device.

The device connects to Cisco SD-WAN Controller s 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

Decommissions a device from the network by detaching templates, disabling the WAN interface, invalidating the device, and removing it from the controller list.

From Cisco SD-WAN Manager Release 20.9 and later, follow these steps to remove a device that was onboarded using a generic bootstrap configuration from SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Locate the device you want to remove in the list.
3. Click **Invalid** in the **Validate** column for that device, and confirm the action in the dialog box to invalidate the device.
4. Click **Send to Controllers** to synchronize the updated WAN Edge list with all controllers.
5. From the SD-WAN Manager menu, choose **Configuration** > **Devices**.
6. Locate the device in the list, click the **...**icon and choose **Delete WAN Edge**.
7. Click **OK** in the dialog box to permanently remove the device from the network.

On-Site bootstrap process for Cisco IOS XE Catalyst SD-WAN devices

Facilitates the initial network connectivity of a device by loading a bootstrap configuration file from a USB drive or internal boot flash. This process enables automated provisioning for devices supporting Cisco Catalyst SD-WAN.

The on-site bootstrap process is a provisioning method that uses a configuration file to bring a Cisco IOS XE Catalyst SD-WAN devices onto the network during the boot sequence that

- supports loading from a bootable USB drive,
- supports loading from internal boot flash, and
- prioritizes boot flash configuration if files exist in both locations.

On-Site bootstrap workflow

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

1. Use Cisco SD-WAN Manager to generate a configuration file.
2. 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.
3. Boot the device.

Restrictions for on-site bootstrap process

Describes limitations for the on-site bootstrap process on Cisco Catalyst SD-WAN devices. These restrictions ensure successful device onboarding and network connectivity.
No support configuring cellular interfaces or other NIM module

Onboarding using a bootstrap file does not support configuring cellular interfaces or other NIM module-specific configurations.

Does not work for features that require side encryption

Avoid including features that require Cisco SD-WAN Manager side encryption in the bootstrap file, as this can cause bootstrap and PNP failure.

- Cisco SD-WAN Manager and the device cannot share the same secret keys.
- Do not use Cisco SD-WAN Manager encrypted configuration in bootstrap directly on the device.

Perform the on-site bootstrap process for Cisco Catalyst SD-WAN devices

Configure the on-site bootstrap process for Cisco Catalyst SD-WAN devices. This process enables devices to load configuration from a USB drive or bootflash and come up on the network.

The purpose of this task is to enable Cisco Catalyst SD-WAN devices to be bootstrapped on-site by loading a configuration file from a USB drive or internal bootflash. This allows the device to join the network with the required settings.

- Generate a bootstrap configuration file using SD-WAN Manager.
- Load the configuration file onto the device using USB drive or bootflash.

This task is relevant when deploying Cisco Catalyst SD-WAN devices in environments where network connectivity is not available for remote onboarding, or when a device must be configured locally using a bootstrap file.

The on-site bootstrap process consists of generating a configuration file, transferring it to the device, and booting the device so it loads the configuration and joins the network.

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

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

- A supported SD-WAN Manager image is installed on the device.
- The device is in its factory state with no added configuration.
- From the SD-WAN Manager menu, choose **Administration** > **Settings** and ensure there is an appropriate Organization Name and the Cisco Catalyst SD-WAN Validator IP address.

Follow these steps to perform the on-site bootstrap process for Cisco Catalyst SD-WAN devices:

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. If you are using your own enterprise root certificate authority (CA) for device certification in your network, take these actions in SD-WAN Manager:
   a) From the 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**.
3. From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
4. Click **Feature** > **Templates** and create a template for the device. Perform the following steps:
   a) From the 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.

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

5. 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 7.

   > **Note**
   >
   > For hardware devices, use the bootstrap file name as `ciscosdwan.cfg`. This file is generated by 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`.

6. 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.

7. Copy the `ciscosdwan.cfg` file to a bootable USB drive or to the bootflash of the device. If you are using a USB drive, plug the USB drive into the device.

   > **Note**
   >
   > The file name must be exactly the same as shown above or the device will not read it.

8. 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 gives priority to a configuration file that is on its bootflash.

After completing these steps, the device will load the configuration file from the USB drive or bootflash and come up on the network with the required settings. The device will be ready for further configuration or operation as needed.

- If you need to configure cellular interfaces or NIM module-specific configurations, push a full configuration after onboarding.

3 Firewall Ports for Cisco Catalyst SD-WAN Deployments

Topics:

- Cisco Catalyst SD-WAN-specific port terminology
- Port offset
- Port hopping
- Effects of port hopping
- Ports used by Cisco vEdge Devices
- Ports used by Cisco Catalyst SD-WAN devices running multiple vCPUs
- Administrative ports used by Cisco SD-WAN Manager
- Configure the port offset
- Perform port hopping manually

Describes the ports used by SD-WAN devices for communication and the necessary firewall configurations to enable traffic exchange.

Cisco Catalyst SD-WAN-specific port terminology

Explains the default port configuration used by Cisco vEdge devices for control and traffic connections in overlay networks.

Cisco Catalyst SD-WAN-specific port terminology is a networking configuration that uses base port 12346 for establishing connections that handle control and traffic in the overlay network.

NAT gateway considerations

NAT gateway configurations can affect port assignments in specific scenarios.

> **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

Explains how to configure different port numbers for multiple devices behind a single NAT device.

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.

Port offset configuration details

The port offset can be a value from 0 through 19. The default port offset is 0.

For example, if you configure a device with a port offset of 1, that device uses port 12347.

For NAT devices that can differentiate among the devices behind the NAT, you do not need to configure the port offset.

Port hopping

Describes the process by which devices try different ports when establishing connections in an overlay network.

Port hopping is a connection establishment process that

- enables devices to try different ports when attempting to establish connections with each other if the first port fails, and
- rotates through a total of five base ports with increasing wait times between connection attempts.

After a failure, the port value is incremented and the connection attempt is retried.

Port hopping operation

In the context of a Cisco Catalyst SD-WAN overlay network, the software rotates though a total of five base ports, waiting longer and longer between each connection attempt.

Default port configuration:

- 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.

Device behavior with port hopping:

- 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.

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.

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 this 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 this command:

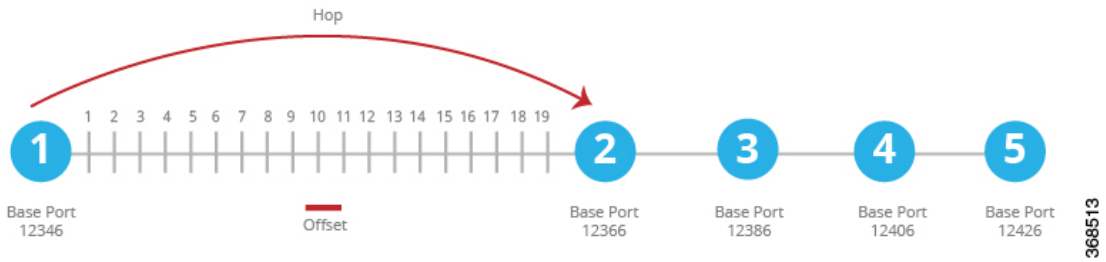
```
system
 no port-hop
```

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.

Cisco vEdge Device port hopping sequence

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.

Figure 1: Example of Cisco vEdge Device Port Hopping



Effects of port hopping

Explains the impacts of port hopping on control plane connections and BFD sessions when controller devices experience failures and recovery.

Port hopping effects are network behaviors that

- cause control connections and BFD sessions to shut down and restart when controller devices recover from failures
- occur when devices attempt to re-establish connections by switching to different ports, and
- impact the stability of the overlay network control plane during recovery scenarios.

Port hopping behavior details

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.

> **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.

Port hopping scenarios

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.

Ports used by Cisco vEdge Devices

Lists the ports used by Cisco vEdge devices for DTLS control plane connections and IPsec data plane connections in overlay networks.

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

Provides port allocation information for Cisco Catalyst SD-WAN devices configured with multiple virtual CPUs for control connections.

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.

This 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

Lists the administrative ports that Cisco SD-WAN Manager uses for protocol-specific communication and cluster operations.

Cisco SD-WAN Manager uses administrative ports for protocol-specific communication and cluster operations. This reference provides the port specifications for network administrators and system integrators.

Protocol-specific communication ports

Cisco SD-WAN Manager uses these 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
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

Cluster communication ports

Cisco SD-WAN Manager clusters use these 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

Cisco SD-WAN Manager Service	Traffic Direction	Protocol	Port Numbers
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

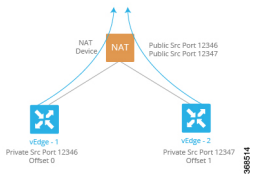
Configure the port offset

Configure a port offset when multiple Cisco vEdge devices are behind the same full-cone NAT device to avoid port conflicts.

The purpose of configuring a port offset is to avoid port conflicts when multiple Cisco vEdge devices are deployed behind the same full-cone NAT device.

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. The port offset can be a value from 0 through 19. The default port offset is 0.

Figure 2: Example of port offset configuration



Configure the port offset on the device.

```
Device(config)# system port-offset number
```

The port offset is configured. In the example where vEdge-1 uses the default port offset of 0 and vEdge-2 has a port offset of 1:

- 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

Configure a Cisco vEdge device to perform port hopping manually using the request port-hop command.

This task allows you to manually initiate port hopping on a Cisco vEdge device, which can help restart control connections and resolve BFD startup issues.

Port hopping is useful when the router's control connections are up but BFD is not starting. The command restarts control connections on the next port number, allowing BFD to start properly.

Request port hopping on the Cisco vEdge device:

```
vEdge# request port-hop
```

The **request port-hop** command restarts the control connections on the next port number, and BFD should then also start.

4 Onboarding Cisco SD-WAN Manager

Topics:

- Cisco SD-WAN Manager personas
- Storage devices
- Software download process
- Feature history for device software installation
- Platform support
- Cisco IOS XE image compatibility
- Self-signed trustpoint
- Autonomous and controller modes
- Restrictions for installing and upgrading device software
- Software Installation for Cisco IOS XE Routers
- Plug and Play onboarding
- Plug and Play onboarding workflow
- Non-Plug and Play onboarding
- Mode discovery and mode change with a bootstrap file
- Reset a device to a Controller mode day zero configuration using CLI commands
- Configuration persistence during mode switch
- Verifying Controller and Autonomous modes
- Change the console port access after installation, in Controller mode
- Restoring Smart Licensing after switching modes
- Deploy a Cisco SD-WAN instance
- Create a Cisco SD-WAN manager VM instance on VMware ESXi
- Cisco SD-WAN Manager VM Instance on KVM
- Configure Cisco SD-WAN manager

Introduces the process for onboarding Cisco SD-WAN Manager, detailing initial setup steps and requirements.

Cisco SD-WAN Manager personas

Explains how Cisco SD-WAN Manager personas and storage devices are selected and assigned during initial server deployment, including their roles and configuration options.

A Cisco SD-WAN Manager persona is a server attribute that

- defines which services run on the server, and
- defines the role that the server has in a Cisco SD-WAN Manager cluster.

Types of Cisco SD-WAN Manager personas

The following personas are supported for Cisco SD-WAN Manager:

- Compute + Data: Includes all services required for Cisco SD-WAN Manager, including application, statistics, configuration, messaging, and coordination. Use for standalone nodes and the first node in a cluster.
- Compute: Includes application, configuration, messaging, and coordination services. Does not include statistics services. Must be part of a cluster.
- Data: Includes only application and statistics services. Must be part of a cluster.

To select a persona during initial boot, follow these steps:

1. When prompted, type **1** for Compute + Data, **2** for Compute, or **3** for Data.
2. Confirm your choice by typing **y** at the **`Are you sure`** prompt.

Cluster deployments support the following node combinations:

- Three Compute + Data nodes
- Three Compute + Data nodes and three Data nodes
- Three Compute nodes and three Data nodes (supported only in upgrades from existing deployments)

> **Note**
>
> The persona configured for a Cisco SD-WAN Manager server cannot be changed after initial setup.

Example

The command line prompt for persona selection appears as follows:

```
1) COMPUTE_AND_DATA
2) DATA
3) COMPUTE
Select persona for vManage (1, 2 or 3):
```

To select Compute + Data, type **1**. To select Compute, type **3**. To select Data, type **2**. Confirm your choice with **y** at the **`Are you sure`** prompt.

Storage devices

Introduces storage devices for the vManage server, and guides you through assigning and formatting a storage device during initial setup, including selection and optional formatting steps.

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.

Assigning and formatting a storage device

Each Cisco SD-WAN Manager server has a storage device assigned to it.

The first time after Cisco SD-WAN Manager is installed and boots up, you are prompted to choose a storage device for the Cisco SD-WAN Manager server.

The command line displays the storage device assignment prompt:

```
Available storage devices:
```

A list of available storage devices follows the prompt, with each device preceded by a number. Type the number corresponding to the storage device you want to use for the server.

After you select a storage device, the system asks if you want to format it.. Type **y** to format the storage device, or type **n** to skip formatting. Formatting the storage device permanently deletes all existing data on it.

Software download process

Provides the steps and information required to download Cisco Catalyst SD-WAN software and related components from the Cisco Software Download site.

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.

Table 2: Software components and download notes

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.

Table 3: Software image file name changes

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

Feature history for device software installation

History of features that relate to installing and upgrading the software of network devices.

This table describes the history of features that relate to installing software on network devices.

Table 4: 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.
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.

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.

Platform support

Describes the platforms that support the installation and upgrade procedures described here.

Describes the platforms that support the installation and upgrade procedures described here.

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)
- 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

Which software image types to use for platforms operating in Cisco Catalyst SD-WAN.

Describes which software image types to use for platforms operating in Cisco Catalyst SD-WAN.

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).

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.

Describes the self-signed trustpoint that is generated and loaded to a device when it boots up.

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.

Autonomous and controller modes

Two installation modes are available.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.

Describes the two installation modes that are available on devices. Autonomous mode supports the functionality of Cisco IOS XE in a non-Cisco Catalyst SD-WAN deployment and Controller mode supports the Cisco Catalyst SD-WAN solution.

Table 5: Comparison of modes

Feature	Autonomous Mode	Controller Mode
Configuration method	• Command Line Interface (CLI) • NETCONF	YANG-based configuration • Cisco SD-WAN Manager • NETCONF

Feature	Autonomous Mode	Controller Mode
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)
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

Restrictions for installing and upgrading device software

Restrictions relevant for installing and upgrading software on devices in a Cisco Catalyst SD-WAN environment.

Describes restrictions relevant for installing and upgrading software on devices in a Cisco Catalyst SD-WAN environment.

Dual-IOSd

Dual-IOSd is supported only in autonomous mode.

Requirement of universalk9 images

Software 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.

Changing mode clears configuration

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

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, the WebUI is not supported, and an error message is displayed if used.

Keep existing image

When upgrading, do not delete the existing image. This provides a software rollback option.

If upgrade fails

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.

Upgrading a device to to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

When upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from Cisco IOS XE Releases 17.3.1a or earlier, do not make any changes to the device configuration using CLI commands 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 commands, the device can have inconsistent configuration and the upgrade fails. If you perform the upgrade 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, upgrade the device using Cisco Catalyst SD-WAN.

Firmware upgrade: primary and backup tunnel interfaces

From 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, refer to the **vmanage-connection-preference** command in the *Cisco Catalyst SD-WAN Command Reference Guide*. Configuring an interface with a higher preference value gives the interface a higher priority.

Downgrading devices to releases earlier than 17.1.x

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.

Software Installation for Cisco IOS XE Routers

Software installation for different platforms, in the context of Cisco Catalyst SD-WAN.

Describes software installation for different platforms, in the context of Cisco Catalyst SD-WAN.

Software image type

Software image type to download.

Describes the software image type to download.

For devices operating with Cisco Catalyst SD-WAN, the software image to use has a filename in this pattern:

<router-model>-universalk9.<release-number>

Images are available on the Cisco Software Download site.

Installing software on select platforms

Provides links to documents for information about installing software on specific platforms.

Provides links to documents for information about installing software on specific platforms.

Refer to these documents for installation instructions:

- 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 the Cisco Catalyst 8000V Edge Software platform

Information about installing software on the Cisco Catalyst 8000V Edge software platform.

Provides information about installing software on the Cisco Catalyst 8000V Edge software platform.

From 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.

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*.

Software image

Use 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

Controller mode

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.

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.

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.

Install software on the Cisco CSR 1000v platform

Links to detailed information about installing software on the Cisco CSR 1000v platform.

Provides links to detailed information about installing software on the Cisco CSR 1000v platform.

Based on the cloud service in which you are deploying the CSR 1000v instance, see this information about performing the bootstrap or the day 0 configurations:

- 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

Plug and Play onboarding

Information about onboarding devices through Cisco Plug and Play.

Provides information about onboarding devices through Cisco Plug and Play.

Plug and Play onboarding workflow

Steps for onboarding devices to Cisco Catalyst SD-WAN using Plug and Play.

Note these considerations regarding Plug and Play:

- 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.
- 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.

For more information, refer to the Plug and Play Support Guide.

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.

Mode discovery with Plug and Play onboarding

The PnP-based discovery process determines the mode in which the device operates, and initiates a mode change if required.

Describes how the Plug and Play (PnP)-based discovery process determines the mode and changes it if necessary.

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change if necessary. The mode change causes the device to reboot. After the reboot, the device performs the appropriate discovery process.

When you upgrade to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, on a Cisco device running an earlier verion of Cisco IOS XE or a Cisco Catalyst SD-WAN image, the device starts in Autonomous mode or Controller mode depending on the configured controller.

Deployment using Plug and Play (PnP) may include any of these discovery process scenarios:

Table 6: PnP discovery process scenarios

Bootup 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

Describes how a device can automatically learn about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets.

Describes how a device can automatically learn about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets.

How a device receives IP address and gateway server information during PnP onboarding

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.

Automatic IP address detection applies only to day zero deployments and is enabled by default.

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.

IP address not preserved after reboot

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.

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.

Restrictions for automatic IP address detection

- Automatic IP address detection 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.
- Automatic IP address detection is supported only on devices that are in Controller mode, for configuration by Cisco Catalyst SD-WAN.
- Automatic IP address detection 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.
- Automatic IP address detection 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-Plug and Play onboarding

How to onboard devices to Cisco Catalyst SD-WAN without using Plug and Play (PnP).

Describes how to onboard devices to Cisco Catalyst SD-WAN without using Plug and Play (PnP).

New installation: Mode change device day zero scenario

A prerequisite for this process is a bootstrap file.

For software devices such as Cisco Catalyst 8000V Edge Software, 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.

Describes the process by which a new device determines which mode to use (Autonomous or Controller) and boots up.

1. If a 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 device determines if a mode change is required, based on the bootstrap file, and boots up.

- If the ciscosdwan.cfg or ciscosdwan_cloud_init.cfg bootstrap files are available 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.

  The bootstrap file (ciscosdwan.cfg) is generated by Cisco SD-WAN Manager, and has a UUID, but no OTP.

- If a ciscortr.cfg bootstrap file or config-wizard is discovered, mode change is not initiated and the boot up continues in Autonomous mode.

Change a device to Autonomous mode

Procedure for changing a device to Autonomous mode.

Use the **controller-mode disable** command only to temporarily change the device to Autonomous mode. Return the device to Controller mode using the same image.

> **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.

1. Use the **controller-mode reset** command to take the device back to the day zero configuration.

```
Device# controller-mode reset
```

2. Use the **controller-mode disable** command to switch the device to Autonomous mode.

```
Device# controller-mode disable
```

Change a device to Controller mode

Procedure for changing 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.

> **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.

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.
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. Verify that the device expanded the image file.

Viewing the sdwaninstaller directory

Conditions in which you cannot view the contents of the sdwaninstaller directory.

Describes conditions in which you cannot view the contents of the sdwaninstaller directory.

You cannot view the contents of the bootflash:/.sdwaninstaller directory or .sdwanistallerfs file of a Cisco IOS XE Catalyst SD-WAN device in either of these 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 possible when the file and directory are hidden.

Mode discovery and mode change with a bootstrap file

Explains mode discovery and mode change with a bootstrap file.

Describes mode discovery and mode change using a bootstrap file.

Preventing a device from booting in Controller mode

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 Controller mode. To prevent the device from booting up in Controller mode, before performing the device upgrade, ensure that you remove the stale Cisco Catalyst SD-WAN configuration file from the bootflash, and delete all artifacts of Cisco Catalyst SD-WAN from the bootflash.

To delete all the artifacts:

- 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

Configuration file prerequisites for mode change
Table 7: Configuration file prerequisites

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

Upgrading a device already running a Cisco Catalyst SD-WAN image

On a device that is already running 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.

Booting Cisco CSR 1000v and Cisco Catalyst 8000V devices in Controller mode

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

Reset a device to a Controller mode day zero configuration using CLI commands

Describes how to reset a device to a Controller mode day zero configuration using a CLI command.

Erase the Cisco Catalyst SD-WAN configuration of the current active image to a reset a device to a Controller mode day zero configuration.

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 performing the configuration reset operation.

> **Note**
>
> Failure to follow save the bootstrap file in these environments causes loss of virtual machine connectivity.

1. To erase the Cisco Catalyst SD-WAN configuration of the current active image, use the **request platform software sdwan config reset** CLI command

```
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.
```

2. Reload the router after running the CLI command.

Executing this CLI command ensures the configuration for the currently installed version is wiped, together with crypto keys. The device enters the day zero workflow after the reload.

One of these occurs next:

- If the device is set up to use PnP for onboarding, then PnP discovery begins.
- 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.

Configuration persistence during mode switch

Configuration retention and erasure when switching a device between Autonomous and Controller modes.

Describes configuration retention and erasure when switching a device between Autonomous and Controller modes.

Table 8: Mode switch behavior

Current configuration mode	Switching to	Behavior
Autonomous	Controller	Erases the contents of NVRAM and the startup configuration. Device reverts to a day zero configuration. The previous running configuration is stored in bootflash. The configuration is not restored. **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 can manually restore the configuration from a backup.
Controller	Autonomous	Erases the ConfD configuration database (CDB) contents, for subsequent mode switches, and the Cisco IOS XE configuration is not restored, as the startup configuration is empty. You can manually restore the configuration from a backup.

Verifying Controller and Autonomous modes

The **show** commands to use on a device to verify Controller or Autonomous mode.

Describes the **show** commands to use on a device to verify Controller or Autonomous mode.

Verifying 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 a device is in Controller mode, the **show sdwan running-config** command does not display this 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.

Verifying 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
```

Change the console port access after installation, in Controller mode

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.

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.

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 these options to configure the type of access:
   - virtual: This option specifies that the device is accessed through the hypervisor virtual VGA console.
   - 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 **platform console serial** command to the CLI add-on profile or CLI add-on template. This helps prevent Cisco SD-WAN Manager from 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.

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
```

This step reboots the device in controller mode.

Restoring Smart Licensing after switching modes

Restoring Smart Licensing authorization lost when a device switches from Autonomous to Controller mode.

Describes methods to restore Smart Licensing authorization lost when a device switches from Autonomous to Controller mode.

When a device swtiches from Autonomous mode to Controller mode and back to Autonomous mode again, it loses authorization for Smart Licensing.

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.

Restore Smart Licensing

Procedure for enabling Smart License reservation.

1. Configure the device to reach Cisco Smart Software Manager (CSSM).
2. Register the device using the **license smart register idtoken** *token* **force** command in privileged EXEC mode.
3. Set the required crypto throughput using the **platform hardware throughput crypto** *crypto-value* command.
4. Save the configuration using the **write memory** command 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.

Deploy a Cisco SD-WAN instance

Configure a Cisco SD-WAN Manager instance to provide centralized network management for your SD-WAN overlay network. This enables you to monitor, configure, and maintain vEdge routers and links efficiently.

Follow these steps to deploy a SD-WAN instance or cluster:

It is recommended to deploy a Cisco SD-WAN Manager cluster (minimum three instances) for larger networks to ensure high availability and scalability.

1. Create a Cisco SD-WAN Manager VM instance on an ESXi or KVM hypervisor.
2. Create either a minimal or a full configuration for each Cisco SD-WAN Manager instance.

   You can configure Cisco SD-WAN Manager by using the ESXi console, or use SSH to open a CLI session and manually configure Cisco SD-WAN Manager.
3. Configure certificate settings and generate a certificate for 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 a Cisco SD-WAN manager VM instance on VMware ESXi

Configure a Cisco SD-WAN Manager VM instance on a server running VMware vSphere ESXi Hypervisor. This task ensures that you can deploy and start the VM for Cisco SD-WAN Manager with the required resources and connectivity.

Follow these steps to create a Cisco SD-WAN Manager VM instance on ESXi:

Use this task when you need to set up Cisco SD-WAN Manager on an ESXi server. You can also use a server running the Kernel-based Virtual Machine (KVM) hypervisor for deployment. Disk encryption can be enabled on the hypervisor starting from the specified release.

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.

1. Start the vSphere Client and create a Cisco SD-WAN Manager VM instance.
2. Create a new virtual disk with a volume of at least 100 GB for the Cisco SD-WAN Manager database.
3. Add additional vNICs as required.
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.
6. 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

Configure a new virtual disk with a minimum volume of 100 GB for the Cisco SD-WAN Manager database. This ensures sufficient storage for optimal database performance.

Follow these steps to create a new virtual disk with at least 100 GB for the Cisco SD-WAN Manager database:

1. Select the Cisco SD-WAN Manager VM instance in the vSphere Client and click **Edit** virtual machine settings.
2. Click **Add** to add a new virtual disk, then click **OK** in the Virtual Machine Properties screen.
3. Select **Hard Disk** as the device type to add, then click **Next** in the Add Hardware screen.
4. Select **Create a new virtual** disk in the Select a Disk screen, then click **Next**.

5. Specify the disk capacity for the Cisco SD-WAN Manager database as 100 GB in the Create a Disk screen, then click **Next**.
6. Choose IDE (or SCSI for releases starting Cisco vManage Release 20.3.1) as the virtual storage device in the Advanced Options screen, then click **Next**.

   If you are using IDE for releases older than Cisco vManage Release 20.3.1, the virtual store device must be IDE.

7. Click **Finish** in the Ready to Complete screen to complete creating the new virtual disk with a capacity of 100 GB.

The system displays the vSphere Client screen with **Getting Started** selected, indicating the new virtual disk has been created successfully.

Add additional vnics

Configure additional vNICs for the management interface and Message Bus in a vSphere Client VM instance. This task enables enhanced network connectivity and supports cluster communication requirements.

Follow these steps to add additional vNICs for management and Message Bus interfaces:

1. Select the Cisco SD-WAN Manager VM instance in the vSphere Client and click **Edit** virtual machine settings.
2. On the Virtual Machine Properties screen, click **Add** to add a new vNIC for the management interface, then click **OK**.
3. Choose Ethernet Adapter as the device type to add, then click **Next**.
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC, then click **Next**.
5. On the Ready to Complete screen, click **Finish**.
6. When the Virtual Machine Properties screen opens showing 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 for the Message Bus.

Connect a VM instance to the Cisco SD-WAN manager console

Configure a VM instance to connect to the Cisco SD-WAN Manager console. This task enables you to power on the VM, access the console, configure storage and network settings, and log in to the instance for management.

Follow these steps to connect a VM instance to the Cisco 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. Configure an IP address on the Cisco SD-WAN Manager instance to enable web browser access.
   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. Connect to the Cisco SD-WAN Manager instance using a web browser.

```
https:// ip-address :8443/
```

8. Log in to the Cisco SD-WAN Manager instance.

   The default username and password is admin/admin.

Cisco SD-WAN Manager VM Instance on KVM

Explains how to create a Cisco SD-WAN Manager virtual machine (VM) instance on a server running the Kernel-based Virtual Machine (KVM) hypervisor.

A VM instance is a virtualized server environment that

- runs Cisco SD-WAN Manager on a server with hypervisor software
- enables deployment on Kernel-based Virtual Machine (KVM) or VMware vSphere ESXi hypervisors, and
- requires specific server hardware and configuration steps.

Server requirements for VM instances

For server requirements, see Server Hardware Requirements.

Create a VM instance for Cisco SD-WAN Manager on the KVM hypervisor

Configure a Cisco SD-WAN Manager VM instance on the KVM hypervisor to enable network management and orchestration. This task guides you through deploying the VM, configuring storage, hardware, and network interfaces, and preparing the instance for use.

Follow these steps 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.
   - Select **Import existing disk image** radio button.
   - Click **Forward**. The virtual disk is imported and associated to the VM instance you are creating.

4. Provide the existing storage path and click **Browse** to locate the Cisco SD-WAN Manager software image.
   - In the **OS Type** field, select **Linux**.
   - In the **Version** field, select the Linux version that you are running.
   - Click **Forward**.

5. Specify Memory and CPU based on your network topology and number of sites, then click **Forward**.
6. Select Customize configuration before install, and click **Finish**.
7. Select **Disk 1** in the left navigation bar.
   - Click **Advanced Options**.
   - In the Disk Bus field, choose IDE (Cisco vManage Release 20.3.1, choose SCSI).
   - In the **Storage Format** field, choose **qcow2**.
   - 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:
   - 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.
   - In the **Device Type** field, specify IDE disk (Cisco vManage Release 20.3.1, specify SCSI disk) for the virtual storage.
   - In the **Storage Format** field, specify **qcow2**.
   - 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**.
    - In the **Host Device** field, select an appropriate host device.
    - 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 for the Message Bus.
13. In the Cisco SD-WAN Manager Virtual Machine screen, click **Begin Installation**.
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 **admin** and default password **admin**.

    The system prompts you to select the storage device to use.
16. Select **hdc**, which is the new partition 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 SD-WAN manager instance

Configure an IP address on the Cisco SD-WAN Manager instance to enable access using a web browser. Verify that you can log in and reach the instance through the configured network interface.

This task enables you to configure an IP address on the Cisco SD-WAN Manager instance, allowing you to connect to it using a web browser for further management and configuration.

Follow these steps to connect to a Cisco SD-WAN Manager instance:

1. Log in with the default username and password.

```
Login: admin password: admin #
```

2. Configure an IP address on interface eth0 in VPN 512 and add a default route if necessary.

```
# 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
#
```

   Specify an IP address that is reachable on your network to ensure connectivity.

3. Connect to the Cisco SD-WAN Manager instance using a web browser.

```
https://ip-address:8443/
```

4. Log in with the username **admin** and the password **admin**.

You can now access the Cisco SD-WAN Manager instance through your web browser and proceed with further configuration.

After connecting, a guided task flow assists you through the essential configurations for new deployments. For more information, see First Time Settings on Cisco SD-WAN Manager.

Configure Cisco SD-WAN manager

Configure Cisco SD-WAN Manager to enable device authentication and participation in the overlay network. This task ensures that each vManage instance is properly set up using CLI mode and required features are configured for network operation.

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.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Launch the Add Controller and Validator Components workflow.
3. Choose **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.

After completing these steps, each Cisco SD-WAN Manager instance is authenticated and able to join the overlay network. The required features are configured for Cisco SD-WAN Manager operation.

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.

5 Onboarding Cisco SD-WAN Validator

Topics:

- Deploy Cisco Catalyst SD-WAN Validator
- Create Cisco Catalyst SD-WAN Validator VM instance on ESXi
- Create Cisco SD-WAN Validator VM instance on KVM
- Configure the vBond orchestrator
- Add Cisco SD-WAN Validator to the overlay network
- Start the enterprise ZTP server

Introduces the process of onboarding Cisco SD-WAN Validator, guiding users through initial setup and integration steps.

Deploy Cisco Catalyst SD-WAN Validator

Configure the Cisco SD-WAN Validator orchestrator to authenticate controllers and routers, coordinate connectivity, and enable overlay network communication. Verify that the orchestrator is accessible and integrated with Cisco SD-WAN Manager.

Deploying the Cisco SD-WAN Validator orchestrator enables authentication of Cisco SD-WAN Controller controllers and vEdge routers, and coordinates connectivity within the overlay network.

- Establishes secure communication between devices in the overlay network.
- Allows devices behind NAT gateways to connect using a public IP address.

The Cisco SD-WAN Validator orchestrator is a software module that must be accessible to all devices in the overlay network. It is recommended to place it in a DMZ and assign a public IP address for connectivity.

Assigning a public IP address allows Cisco SD-WAN Controller controllers and vEdge routers in private address spaces to establish communication. The orchestrator runs as a VM on a network server and can be located anywhere in the network.

- A Cisco Catalyst SD-WAN overlay network can have one or more Cisco SD-WAN Validators.

Ensure you have access to an ESXi or KVM hypervisor and a network server to host the Cisco SD-WAN Validator VM instance.

- Verify network connectivity and availability of SSH access for configuration.

Follow these steps 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. Use SSH to open a CLI session to Cisco SD-WAN Validator and manually configure 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. Use SSH to open a CLI session to Cisco SD-WAN Validator for the initial configuration. Then create configuration templates on Cisco SD-WAN Manager and attach them to Cisco SD-WAN Validator. When attached, the template parameters overwrite the initial configuration.

After completing these steps, the Cisco SD-WAN Validator orchestrator is deployed, accessible on the network, and integrated with Cisco SD-WAN Manager. Devices in the overlay network can authenticate and communicate securely.

Create Cisco Catalyst SD-WAN Validator VM instance on ESXi

Configure a Cisco Catalyst SD-WAN Validator VM instance on a server running VMware vSphere ESXi Hypervisor. This task enables you to prepare the virtual machine for use as a validator in your Cisco SD-WAN environment.

This task guides you to create a virtual machine instance for Cisco SD-WAN Validator on a server running VMware vSphere ESXi Hypervisor. The VM instance is required to start the validator and integrate it into your SD-WAN deployment.

- Ensure the validator is available for network orchestration and control.

Use this task when you need to deploy a Cisco Catalyst SD-WAN Validator VM instance on a server running ESXi. The procedure is also applicable for servers running KVM Hypervisor software, though the steps may differ.

Disk encryption can be enabled on the hypervisor if required. For server hardware information, see Server Hardware Recommendations.

- If you are using VMware vCenter Server, follow the same procedure, but note that vCenter Server pages may look different than vSphere Client pages.

Before you begin, ensure you have access to a server running VMware vSphere ESXi Hypervisor or KVM Hypervisor software. Review server hardware recommendations and confirm that disk encryption is enabled if needed.

- Refer to Server Hardware Recommendations for server requirements.
- From Cisco Catalyst SD-WAN Control Components Release 20.14.1, disk encryption can be enabled on the hypervisor.

Follow these steps to create a Cisco Catalyst SD-WAN Validator VM instance on ESXi:

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.

Launch vSphere Client and create a Cisco Catalyst SD-WAN Validator VM instance

Configure a Cisco Catalyst SD-WAN Validator VM instance by launching the vSphere Client, deploying the OVF template, and completing the setup steps. This process enables you to create a virtual machine for Cisco SD-WAN validation in your VMware environment.

Follow these steps to launch the 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 ESXi 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 successfully creates the VM instance with the parameters you defined and displays the vSphere Client page with **Getting Started** selected. By default, this includes one vNIC, which is used for the management interface.

Add a vNIC for the tunnel interface

Configure a vNIC for the tunnel interface in a vEdge Cloud VM using the vSphere Client. This task enables connectivity for management and tunnel operations by adding a new virtual network interface card.

Follow these steps to 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

Configure the Cisco Catalyst SD-WAN Validator VM instance and connect to its console. This task enables you to power on the virtual machine and access its console for initial login.

Follow these steps to start the 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 **admin** and the default password **admin**.

See *Configure Cisco Catalyst SD-WAN Validator* for the next steps.

Create Cisco SD-WAN Validator VM instance on KVM

Configure a virtual machine instance for Cisco SD-WAN Validator on a server running the KVM hypervisor. This task enables you to deploy the validator VM for Cisco SD-WAN environments.

Create a virtual machine instance for Cisco SD-WAN Validator on a KVM hypervisor to enable Cisco SD-WAN validation functionality.

- This task allows you to start the validator and prepare it for further configuration.

Use this task when you need to deploy a Cisco SD-WAN Validator VM instance on a server running the Kernel-based Virtual Machine (KVM) hypervisor.

You can also create the VM on a server running vSphere ESXi hypervisor software. For server information, see *Server Hardware Recommendations*.

- This task is relevant for Cisco SD-WAN deployments requiring a validator VM.

Ensure you have access to a server running KVM hypervisor and the Cisco SD-WAN Validator software image.

- Verify server hardware meets requirements as described in *Server Hardware Recommendations*.

Follow these steps 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 for the Cisco SD-WAN Validator instance.
   - Choose **Import existing disk image** option to install the operating system.
   - Click **Forward**.

4. For **Provide the existing storage path**, click **Browse** to find the Cisco SD-WAN Validator software image.
   - For **OS Type**, choose **Linux**.
   - For **Version**, choose the Linux version that you are running.
   - Click **Forward**.

5. Specify Memory and CPU based on your network topology and the number of sites, then click **Forward**.

6. Check **Customize configuration before install** and click **Finish**.
7. Choose **Disk 1** in the left navigation bar.
   - Click **Advanced Options**.
   - For **Disk Bus**, choose **IDE**.
   - For **Storage Format**, choose **qcow2**.
   - Click **Apply** to create the VM instance with the parameters you had defined. By default, this includes one vNIC 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**.
   - In the **Host Device**, choose an appropriate **Host device**.
   - 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**.
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 **admin** and default password **admin**.

After completing these steps, a Cisco SD-WAN Validator VM instance is created and ready for further configuration in your Cisco SD-WAN environment.

See *Configure Cisco Catalyst SD-WAN Validator* for next steps.

- Proceed to configure the validator VM as required for your deployment.

Configure the vBond orchestrator

Configure the vBond orchestrator to enable device authentication and integration into the overlay network. This process includes initial CLI setup, system IP assignment, WAN interface configuration, and preparation for template-based management.

Configure the vBond orchestrator to provide essential authentication and orchestration functions in the overlay network. This task ensures that vBond is reachable, properly identified, and ready for device onboarding and management.

- Enable device authentication and verification for overlay network participation.
- Prepare vBond for management via configuration templates in vManage.

Follow these steps to configure the vBond orchestrator for initial operation in the overlay network:

The vBond orchestrator is a critical component in Cisco SD-WAN deployments, responsible for authenticating and verifying devices before they join the overlay network. This task is performed after deploying the vBond VM or hardware and before attaching configuration templates from vManage.

Use this procedure when setting up a new vBond instance or reinitializing an existing one to factory defaults.

- Perform this configuration before onboarding other devices to the overlay network.

Ensure the vBond VM or hardware is deployed and powered on in your overlay network environment. You must have SSH access to the vBond device and the default admin credentials.

- vBond must have a public IP address for overlay network connectivity.
- Default username and password are both **admin**.

1. Open a CLI session to Cisco SD-WAN Validator 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 recommended. The hostname appears in the CLI prompt and on various Cisco SD-WAN Manager screens to identify 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 for configuration management.

6. Configure the IP address of Cisco SD-WAN Validator as a public address.

   ```
   vBond(config-system)#vbond ip-address local
   ```

   In Releases 16.3 and later, the address can be IPv4 or IPv6. In earlier releases, it must be IPv4. The **local** option designates the device as vBond, not a vEdge router. vBond must run on a standalone VM or hardware router.

   The IP address must be a public address so that all devices in the overlay network can reach Cisco SD-WAN Validator.

7. Configure a time limit for confirming a software upgrade is successful.

   ```
   vBond(config-system)#upgrade-confirm minutes
   ```

   The time can be from 1 through 60 minutes. If confirmation is not received within the configured time, the device 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 WAN transport network.

```
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
```

In Releases 16.3 and later, the IP address can be IPv4 or IPv6. In earlier releases, it must be IPv4. Ensure the prefix for the interface contains the IP address configured in the **vbond local** command.

> **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
```

12. After the overlay network is operational, create a vBond configuration template on Cisco SD-WAN Manager containing the initial configuration parameters.

- System feature template: configure hostname, system IP address, and vBond functionality.
- AAA feature template: configure a password for the "admin" user.
- VPN Interface Ethernet feature template: configure the interface in VPN 0.

It is also recommended to 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.

After completing this task, the vBond orchestrator is configured with a public IP address, system parameters, and WAN connectivity. The device is ready for integration into the overlay network and further management via vManage configuration templates.

Below is an example of a simple configuration on Cisco SD-WAN Validator. This configuration includes several factory-default and default 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
 !
!
```

See *Add Cisco SD-WAN Validator to the Overlay Network* for next steps.

Add Cisco SD-WAN Validator to the overlay network

Guides you through adding a Cisco SD-WAN validator to the overlay network, including making the manager aware of the validator and handling authentication certificate signing, with manual, automatic, and deferred signing options.

After you create a minimal configuration for SD-WAN Validator, you must add it to overlay network by making SD-WAN Manager aware of the validator. When you add SD-WAN Validator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Launch the Add Controller and Validator Components workflow.
3. Choose **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.

Start the enterprise ZTP server

Outlines how to configure an enterprise ZTP server to provide WAN edge devices with necessary IP and root CA information, and explains scenarios where a top-level validator is not required when using the hosted service.

If you are hosting the Cisco Catalyst SD-WAN zero-touch-provisioning (ZTP) server in your enterprise, you must configure one SD-WAN Validator to perform this role. This SD-WAN Validator provides the WAN edge devices in the overlay network with the IP address of your enterprise SD-WAN Validator and with the enterprise root CA chain.

If you are using the Cisco Catalyst SD-WAN ZTP hosted service, there is no need to set up a top-level SD-WAN Validator.

Requirements for ZTP

To start the SD-WAN Validator software, you need the following hardware and software components:

- A WAN edge device on which the SD-WAN Validator software has been installed or the 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, a CSV file that contains the WAN edge device chassis information required by the SD-WAN Validator that is acting as the ZTP server. Each row in the CSV file must contain the following information for each 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.

  - WAN edge device chassis number
  - WAN edge device serial number
  - Validity (either valid or invalid)
  - SD-WAN Validator IP address
  - 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, a JSON file that contains the router chassis information that the 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)
  - SD-WAN Validator IP address
  - 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 SD-WAN Controller release that you are using for SD-WAN Manager, SD-WAN Controller, and 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:

```
validator# 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.

```
validator# 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 device information manually using the **request device** command.

Configure a Router to be a ZTP Server

1. Boot the WAN edge device.
2. Use a console cable to connect a PC to the device.
3. Log in to the device using the default username, which is **admin** , and the default password, which is **admin**. The CLI prompt is displayed.
4. Configure the device to be a top-level SD-WAN Validator :

```
Validator# config
Validator(config)# system vbond ip-address
                    local ztp-server
```

The IP address must be a public address so that the SD-WAN Validator is reachable by all SD-WAN Controllers and devices through the transport network. The **local** option indicates that this device is acting as the SD-WAN Validator. It is this option that starts the SD-WAN Validator software process on the device. The **ztp-server** option establishes this SD-WAN Validator as the ZTP server.

5. Configure an IP address for the interface that connects to the transport network:

```
Validator(config)# vpn 0 interface ge slot /port
validator(config-ge)# ip address prefix /length
validator(config-ge)# no shutdown
```

6. Commit the configuration:

```
validator(config)# commit
```

7. Exit configuration mode:

```
validator(config)# exit
```

8. Verify that the configuration is correct and complete.

```
validator# 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.

```
Validator_ztp# request csr upload home/admin/vbond_ztp.csr
```

10. Sign CSR manually and generate certificate via PNP Connect Cisco PKI.
11. Install certificate.

```
validator_ztp# request certificate install/home/admin/vbond_ztp.cer
```

12. Ensure Cisco IOS XE Catalyst SD-WAN has Cisco root-ca-cert in root-ca chain.
13. Check clock on validator_ZTP and Cisco IOS XE Catalyst SD-WAN .
14. Upload the JSON file that contains the router chassis information to the ZTP server:

```
Validator# 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:

```
Validator# show ztp entries
Validator# show orchestrator valid-devices
```

Here is an example of the configuration of a top-level SD-WAN Validator :

```
validtaor# 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
!
```

.

6 Onboarding Cisco SD-WAN Controller

Topics:

- Deploy a Cisco Catalyst SD-WAN Controller controller
- Create Cisco Catalyst SD-WAN Controller VM instance on ESXi
- Create a Cisco SD-WAN Controller VM instance on KVM
- Configure the Cisco Catalyst SD-WAN Controller
- Add Cisco SD-WAN Controller to the overlay network

Introduces the process for onboarding a Cisco SD-WAN controller, outlining key steps required to integrate the controller into your network.

Deploy a Cisco Catalyst SD-WAN Controller controller

Configure a Cisco SD-WAN Controller controller to establish centralized control in the Cisco Catalyst SD-WAN overlay network. This process ensures the controller is operational and integrated with the network for effective routing and policy management.

Deploying a Cisco SD-WAN Controller controller establishes the centralized control plane for the Cisco Catalyst SD-WAN overlay network, enabling centralized routing and policy enforcement.

The Cisco SD-WAN Controller controller is a core component of the Cisco Catalyst SD-WAN overlay network, maintaining a centralized routing table and policy. It connects to each vEdge router via DTLS and runs as a virtual machine on a network server.

An overlay network can have one or more Cisco SD-WAN Controller controllers for redundancy and scalability. A single controller supports up to 2,000 control sessions, and a Cisco SD-WAN Manager or Cisco SD-WAN Manager cluster can support up to 20 controllers.

Ensure you have access to an ESXi or KVM hypervisor and the necessary resources to deploy a Cisco SD-WAN Controller virtual machine.

Follow these steps to deploy a Cisco SD-WAN Controller controller:

1. Create a Cisco SD-WAN Controller VM instance on an ESXi or KVM hypervisor.
2. Create a minimal configuration for the Cisco SD-WAN Controller to allow network accessibility. Use SSH to open a CLI session and manually configure 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 by creating a Cisco SD-WAN Manager template and attaching it to the controller. Attaching the template overwrites the initial minimal configuration.

The Cisco SD-WAN Controller controller is deployed, accessible on the network, and integrated with the Cisco Catalyst SD-WAN overlay for centralized routing and policy management.

Create Cisco Catalyst SD-WAN Controller VM instance on ESXi

Configure a Cisco Catalyst SD-WAN Controller VM instance on a server running VMware vSphere ESXi Hypervisor. This task enables you to start the Cisco SD-WAN Controller and connect to its console for further configuration.

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 task 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.
- From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can enable disk encryption on the hypervisor.

This task is relevant when deploying a Cisco SD-WAN Controller VM instance for Cisco SD-WAN environments using VMware vSphere ESXi Hypervisor.

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.

- For server requirements, see Server Hardware Recommendations.

Ensure you have access to a server running VMware vSphere ESXi Hypervisor and have downloaded the vsmart.ova file from Cisco.

- Verify that your server meets the hardware requirements for deploying the VM instance.

Follow these steps to create a Cisco Catalyst SD-WAN Controller VM instance on ESXi:

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.

After completing these steps, the Cisco SD-WAN Controller VM instance is created and started on ESXi. You can connect to its console and proceed with further configuration.

Refer to the configuration guide for Cisco Catalyst SD-WAN Controller for next steps.

- See *Configure Cisco Catalyst SD-WAN Controller*.

Launch vSphere Client and create a Cisco Catalyst SD-WAN Controller VM instance

Configure a Cisco Catalyst SD-WAN Controller VM instance by launching the VMware vSphere Client and deploying the OVF template. This process enables you to create a virtual machine with the required parameters for your deployment.

Follow these steps to launch the 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 successfully creates the VM instance with the parameters you defined and displays the vSphere Client page with **Getting Started** selected. By default, this includes one vNIC, which is used for the tunnel interface.

Add a vNIC for the management interface

Configure a vNIC for the management interface in the vSphere Client. This task enables management connectivity for the Cisco SD-WAN Manager VM instance.

Follow these steps to 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

Configure the Cisco Catalyst SD-WAN Controller VM instance and connect to its console. This task enables you to access the virtual machine for initial setup and management.

Follow these steps to start the 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**.

See *Configure Cisco Catalyst SD-WAN Controller* for next steps.

Create a Cisco SD-WAN Controller VM instance on KVM

Configure a Cisco SD-WAN Controller VM instance on a server running the KVM hypervisor. This enables you to deploy the Cisco SD-WAN Controller controller in your virtualized environment.

This task describes how to create a Cisco SD-WAN Controller virtual machine instance on a server running the KVM hypervisor, enabling the deployment of the Cisco SD-WAN Controller controller in a virtualized environment.

Use this task when you need to deploy a Cisco SD-WAN Controller controller as a virtual machine on a server that is running the Kernel-based Virtual Machine (KVM) hypervisor. This is typically required as part of the initial setup or scaling of your Cisco SD-WAN environment.

You can also create the VM on a server running the VMware vSphere ESXi Hypervisor software. For server requirements, see *Server Hardware Recommendations*.

Ensure you have access to a server running the KVM hypervisor and have the Cisco SD-WAN Controller software image available.

Follow these steps to create a Cisco SD-WAN Controller VM instance on KVM:

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 perform the following:

   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 upper-left corner of the screen.
11. Wait for the system to create the virtual machine instance and display the Cisco SD-WAN Controller console.
12. At the login prompt, log in with the default username **admin** and the default password **admin**.

After completing these steps, a Cisco SD-WAN Controller VM instance is created and ready for further configuration in your Cisco SD-WAN environment.

See *Configure Cisco Catalyst SD-WAN Controller* for next steps.

Configure the Cisco Catalyst SD-WAN Controller

Configure the Cisco Catalyst SD-WAN Controller to enable authentication, join the overlay network, and establish basic connectivity. Configure essential parameters such as system IP, site ID, and tunnel interfaces to ensure proper operation.

This task enables you to configure the Cisco Catalyst SD-WAN Controller with the required initial settings so it can be authenticated, verified, and participate in the overlay network. You will set up basic features such as system IP, site and domain IDs, and tunnel interfaces.

- Establishes device identity and connectivity for overlay network participation.
- Prepares the controller for further configuration using templates in Cisco SD-WAN Manager.

Use this task after deploying the Cisco SD-WAN Controller virtual machines in your overlay network. The devices start with a factory-default configuration and require manual setup to join the overlay network and communicate with other controllers and vEdge devices.

Perform this configuration before attaching configuration templates from Cisco SD-WAN Manager. The initial configuration ensures the device can be managed and participate in control plane operations.

- All Cisco SD-WAN Controllers must have identical policies for predictable overlay network operation.

Ensure the Cisco SD-WAN Controller virtual machines are deployed and running with factory-default configuration. You must have SSH access to the device CLI and know the default credentials (username: **admin**, password: **admin**).

- Identify the required IP addresses for system IP, site ID, domain ID, and Cisco SD-WAN Validator.
- Determine the interface in VPN 0 to be used as the tunnel interface, and ensure it connects to a WAN transport network accessible by all vEdge devices.

Follow these steps to configure the Cisco Catalyst SD-WAN Controller for overlay network participation:

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 (optional but recommended).

```
Cisco(config)# system host-name hostname
```

This name appears in the CLI prompt and 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 IPv4 or IPv6. In earlier releases, only IPv4 is supported. Releases 19.1 and later do not allow configuration of IPv6 unique local addresses; use 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, 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 for configuration download.

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 or DNS name of the Cisco Catalyst SD-WAN Validator.

The Cisco Catalyst SD-WAN Validator's IP address must be public to allow all Cisco vEdge devices to reach it.

```
vSmart(config-system)# vbond  (dns-name | ip-address)
```

9. Configure a time limit for confirming that a software upgrade is successful.

The time can be from 1 through 60 minutes. If confirmation is not received within the configured time, the device reverts to the previous software image.

```
vSmart(config-system)# upgrade-confirm minutes
```

10. Change the password for the user "admin".

The default password is "admin".

```
vSmart(config-system)# user admin password password
```

11. Configure an interface in VPN 0 to be used as a tunnel interface.

    VPN 0 is the WAN transport VPN. The tunnel interface carries control traffic among devices in the overlay network. The interface name has the format **eth***number*. Enable the interface and configure its IP address (static or DHCP). In Releases 16.3 and later, both IPv4 and IPv6 are supported for dual-stack operation.

    > **Note**
    >
    > You must configure a tunnel interface on at least one interface in VPN 0 for the overlay network to come up and for Cisco SD-WAN Controller to participate. This interface must connect to a WAN transport network accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

```
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
```

12. Configure a color for the tunnel to identify the type of WAN transport.

    You can use the default color (**default**), or configure a more appropriate color such as **mpls** or **metro-ethernet** depending on the 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
```

16. After the overlay network is operational, create a Cisco SD-WAN Controller configuration template on Cisco SD-WAN Manager containing the initial configuration parameters.

    - System feature template: configure hostname, system IP, and Cisco SD-WAN Validator functionality.
    - AAA feature template: configure password for the "admin" user.
    - VPN Interface Ethernet feature template: configure interface, default route, and DNS server in VPN 0.

It is also recommended to 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. Otherwise, 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.

After completing these steps, the Cisco SD-WAN Controller is configured with the required initial parameters, can participate in the overlay network, and is ready for further configuration using templates in Cisco SD-WAN Manager.

Below is an example of a simple configuration on a Cisco SD-WAN Controller. This configuration includes several settings from the factory-default configuration and shows default 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
 !
!
```

For next steps, see *Add the Cisco SD-WAN Controller to the Overlay Network*.

Add Cisco SD-WAN Controller to the overlay network

Guides you through adding an SD-WAN controller to the overlay network using SD-WAN Manager workflows, including steps for certificate generation, signing, authentication, and handling both manual and automatic certificate renewal options.

After you create a minimal configuration for SD-WAN Controller, you must add it to overlay network by making SD-WAN Manager aware of the controller. When you add SD-WAN Controller, a signed certificate is generated and is used to validate and authenticate the orchestrator.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Launch the Add Controller and Validator Components workflow.

3. Choose **Controller**, 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.

7 Add SD-WAN controller and SD-WAN validator components

Topics:

- Feature history for SD-WAN controller and SD-WAN validator components workflow
- Control components certificate management workflow
- Supported solutions for the add SD-WAN controller and SD-WAN validator workflow
- Supported environments for the add SD-WAN controller and SD-WAN validator components workflow
- Requirements for adding SD-WAN controller and SD-WAN validator components
- Add SD-WAN controllers or SD-WAN validators using a workflow

Provides information about adding SD-WAN Controller and SD-WAN Validator components to your network infrastructure.

Feature history for SD-WAN controller and SD-WAN validator components workflow

Provides the feature history for adding SD-WAN Controller and SD-WAN Validator components.

Table 9: 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.

Control components certificate management workflow

Explains a step-by-step interactive procedure that adds SD-WAN Controller or SD-WAN Validator components to a fabric.

A Control Components Certificate Management Workflow is a step-by-step interactive procedure that

- adds either SD-WAN Controller or SD-WAN Validator components to an SD-WAN fabric, and
- operates within Cisco SD-WAN Manager.

Certificate requirements

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

Lists the supported solutions for the Add SD-WAN Controller and SD-WAN Validator workflow implementation.

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

Lists the supported environments where the Add SD-WAN Controller and SD-WAN Validator components workflow is available.

The workflow is available in Cisco Catalyst SD-WAN environments in which you manage the SD-WAN Control Components.

Requirements for adding SD-WAN controller and SD-WAN validator components

Outlines the requirements for adding SD-WAN Controller and SD-WAN Validator components to your network environment.

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

Configure SD-WAN Controllers or SD-WAN Validators in your network using the Add Controller and Validator Components workflow.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Launch the Add Controller and Validator Components workflow.
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.

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**.

8 First Time Settings for SD-WAN Manager

Topics:

- Feature history for first time settings
- First time settings for SD-WAN Manager
- Enable multitenancy on SD-WAN Manager
- Configure the organization name
- Configure common SD-WAN Control Component network settings
- Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier
- Configure cloud services
- Configure certificate settings
- Add Cisco SD-WAN Controller and Cisco SD-WAN Validator
- Configure SD-WAN Validator IP address
- Configure identity provider settings
- Configure users and access
- Alarm notification settings
- Configure account lockout settings
- Configure a web server certificate for Cisco SD-WAN Manager

Introduces the overall process and requirements for setting up Cisco SD-WAN Manager, establishing a foundation for subsequent configuration and management tasks.

Feature history for first time settings

Introduces the initial settings required for first-time use of Cisco SD-WAN Manager, outlining the setup flow, configuration prerequisites, and key best practices for new deployments.

This feature introduces a task flow to setup all the initial settings by a first time user of Cisco SD-WAN Manager .

Table 10: 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 for SD-WAN Manager

Explains initial configuration concepts and fundamental requirements, equipping administrators with the knowledge to properly understand and plan the first-time setup of Cisco SD-WAN Manager.

First time settings on Cisco SD-WAN Manager refer to the initial configuration process after onboarding that includes

- a guided task flow to assist you through the initial setup.
- option to choose either a **Standard** or **Express** setup.
- a setup button on the toolbar allows toggling the task flow open and close.

Guided task flow

After onboarding, SD-WAN Manager provides a guided task flow for essential configurations, including both mandatory and recommended settings. Using the toolbar options in the setup, you can manage the progress of the task flow. The guided task flow allows you to:

- Mark steps as complete using the **Mark as complete** option.
- Skip optional steps individually with **Skip** or all at once with **Skip remaining**.
- Stop or restart the task flow at any time after configuring mandatory steps.
- While configuring optional steps, return to a specific step using the **Go to this step** option.

After you update all the basic settings, you can mark the guided task flow as **Complete**. The **Monitor** > **Overview** page opens.

Standard setup

You may choose either a **Standard** or **Express** 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. The tables below provide information about system and management setup.

Table 11: System setup

Setting	Category	On-Prem Deployments	Cloud Deployments
Tenancy mode	Mandatory	Yes	NA

Setting	Category	On-Prem Deployments	Cloud Deployments
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 12: Management

Setting	Category	On-Prem Deployments	Cloud Deployments
Identity provider settings	Optional	Yes	Yes
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, complete the steps that are essential for onboarding network devices.

The tables below provide information about system and management setup.

Table 13: 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

Setting	Category	On-Prem Deployments	Cloud Deployments
Certificate settings	Optional	Yes	Yes
Add control component	Optional	Yes	Yes

Enable multitenancy on SD-WAN Manager

Enable multitenancy mode on SD-WAN Manager to support multiple tenants.

For a multitenancy setup with multiple tenants, enable multitenancy mode on SD-WAN Manager .

Once multitenancy is enabled on the SD-WAN Manager , it cannot be migrated back to a single-tenant mode.

1. Configure the tenancy mode.

   Alternatively, from the SD-WAN Manager menu, choose **Administration** > **Settings** > **Tenancy Mode** .

2. Click **Multitenant** .
3. In the **Domain** , enter the domain name of the service provider (for example, multitenancy.com).
4. Enter a **Cluster Id** (for example, cluster-1 or 123456).
5. Click **Save** .

SD-WAN Manager reboots in multitenant mode. When a provider user logs in to SD-WAN Manager, the provider dashboard appears.

Configure the organization name

Configure the organization name before generating a Certificate Signing Request (CSR).

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.

1. Configure the organization name.

   Alternatively, from the SD-WAN Manager menu, choose **Administration** > **Settings** > **Organization Name** .

2. In **Organization Name**, enter the name of your organization. The organization name must be identical to the name that is configured on the SD-WAN Validator.
3. In **Confirm Organization Name**, re-enter and confirm your organization name.
4. Click **Save**.

After the control connections are up and running, the organization name bar is no longer editable.

Configure common SD-WAN Control Component network settings

Configure common or device-specific network settings for Cisco SD-WAN Control Components.

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.

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** .

2. Configure the following parameters:
   a) Configure NTP

Table 14: 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 15: 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 16: 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 17: 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

Field	Description
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 18: 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 19: 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 20: 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 21: 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 22: 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 23: 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.
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.

Field	Description
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.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.

Field	Description
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.
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.

Field	Description
User name	Enter the username. The username can be a string from 1 to 32 characters.

3. Click **Save** .

Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier

Configure Cisco Smart Account credentials to enable connectivity to PnP Connect, Cisco Umbrella portal, and Cisco PKI certificates.

> **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. SD-WAN Manager uses the Cisco Smart Account credentials to connect to:

- PnP Connect
- Cisco Umbrella portal
- Cisco PKI certificates

1. Configure Smart Account credentials.

   Alternatively, from the SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials** .

2. Enter **Username** and **Password** .
3. Click **Save** .

Configure cloud services

Configure Cloud Services settings to enable Cisco SD-WAN Analytics and access for AI Assistant.

To enable Cisco SD-WAN Analytics and access for AI Assistant, configure Cloud Services settings.

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

3. Enter your Cisco Smart Account credentials in the **User ID** and **Password** fields.

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 .

5. (Optional) Enable **Service Access Authorization**
6. Click **Save** .

Configure certificate settings

This section describes how to configure sertificate settings.

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

1. From the SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Choose **Certificate settings**.
   a) Configure the control component certificate authorization settings.

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.

Field	Description
vEdge Cloud	Choose one of the following options to configure the type of Cisco vEdge cloud authorization: • **Automated (Manager signed)** • **Manual (Enterprise CA – recommended)**
Save	Click to save the changes that you made and hide the **WAN Edge Cloud Certificate Authorization** options.
Cancel	Click to discard the changes that you made and hide the **WAN Edge Cloud Certificate Authorization** options.

c) Configure the hardware WAN edge certificate authorization settings

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 24: 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.

Field	Description
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.

3. Click **Save**.

Add Cisco SD-WAN Controller and Cisco SD-WAN Validator

Add SD-WAN Controller and SD-WAN Validator.

1. Add SD-WAN Controller and SD-WAN Validator.

   Alternatively, from the SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components** .

2. Click **Add control component** . Follow the on-screen instructions to onboard SD-WAN Controller and SD-WAN Validator.

Configure SD-WAN Validator IP address

Configure the SD-WAN Validator IP address.

1. Configure the SD-WAN Validator IP address.

   Alternatively, from the SD-WAN Manager menu, choose **Administration** > **Settings** > **Validator**.

2. Enter the DNS name that points to the SD-WAN Validator or the IP address of the SD-WAN Validator and the port number to use to connect to it.
3. Click **Save** .

Configure identity provider settings

Configure identity provider settings to enable SAML authentication for your tenant.

You can configure up to three Identity Provider Settings (IdPs) per tenant and a maximum of three IdPs per provider.

Click **Click here to download the SAML metadata** and save the contents in a text file. This data is used for configuring Okta.

1. Enable an identity provider.

   Alternatively, from the 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.

2. Click **IDP Name** and enter a unique name for your IdP.
3. Click **Domain** and enter a unique domain name for your IdP, for example, okta.com.

   If the domain name already exists, SD-WAN Manager generates an error message.

4. In the **Upload Identity Provider Metadata** section, upload the SAML metadata file you downloaded from your IdP.
5. Click **Save**.

After you configure a new IdP name, domain, and sign out of your current 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 SD-WAN Manager after configuring a new IdP name and domain.

Configure users and access

Configure users, roles, and scopes in vManage to control access and permissions.

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 .

1. Click **Users**.

   Alternatively, from the 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** .

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** .

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

Configure SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

You can configure SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

1. Configure alarm notifications settings.

   Alternatively, from the SD-WAN Manager menu, choose **Administration** > **Settings** > **Alarm notification settings**.

2. To create alarm notifications, click **here** on screen.

   Alternatively, from the SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

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

Configure account lockout settings to enhance security by limiting login attempts and setting inactivity thresholds.

1. Configure account lockout settings.

   Alternatively, from the SD-WAN Manager menu, choose **Administration** > **Settings** > **Account Lockout**.

2. Enable **Inactive days before locked out** .
3. Enable **Inactive days before account locked out**. Enter the number of consecutive inactive days after which SD-WAN Manager locks out a user.

   An inactive day is defined as a day on which a user does not log in to SD-WAN Manager.

   Valid values are 2 through 90.

4. Enter the **Number of failed login attempts before lockout** .

   Possible values: 1 through 3600

   Default: 3600

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, SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes.

   Possibe values: 1 through 60

   Default: 60

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 SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.

7. In the **Lockout Interval (minutes)** field, enter the number of minutes after which SD-WAN Manager automatically resets a locked out user.

Possible values: 1 through 60

Default: 15

Configure a web server certificate for Cisco SD-WAN Manager

Generate and install a web server certificate for secure connections to the Cisco SD-WAN Manager server.

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.

1. Configure web server certificate settings.

   Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Web Server Certificate**.

2. Choose a method for web server authorization.

   Table 25:

SD-WAN Manager signed	
Enterprise (Auto)	
Enterprise(Manual)	

3. If you choose **Enterprise(Manual)**
4. Click **Generate CSR** .
5. Enter these fields:

   Table 26:

Field	Description
Key size (bits)	Choose an option **2048** or **4096**.
Common name	Enter the **common** with the domain name or IP address of the SD-WAN Manager server. For example, the fully-qualified domain name of SD-WAN Manager could be vmanage.org.local.
Organizational Unit	Enter organizational unit name within your organization.
Organization	Enter the organization name as specified by your root CA.
City	Enter the name of the city where your organization is located.
State	Enter the state in which your city is located.
Email	Enter the email address of the organization.
2-Letter country code	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.

Field	Description
SAN DNS names	Enter the Subject Alternative Name(SAN) DNS names. If you enter more than one DNS name, separate each URI with a space or a comma.
Subject Alternative Name (SAN) URIs	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`**.

6. Click **Generate** to generate the CSR.

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 .

9 Quick Connect Workflow

Topics:

- Feature history for the Quick Connect workflow
- Quick Connect workflow for SD-WAN Manager
- Prerequisites for using the Quick Connect Workflow
- Restrictions for the Quick Connect Workflow
- Run the Quick Connect Workflow
- Auto Sync for uploading devices
- Upload devices manually to SD-WAN Manager

Feature history for the Quick Connect workflow

Explains the Quick Connect Workflow, which provides a guided method for onboarding supported WAN edge devices into the Cisco Catalyst SD-WAN fabric.

This feature history lists the method in Cisco SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network.

Table 27: 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 a guided method in SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network. This feature is supported on Cisco IOS XE Catalyst SD-WAN device s only.
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.

Quick Connect workflow for SD-WAN Manager

This topic explains the Quick Connect workflow in SD-WAN Manager, which creates a basic day-0 configuration profile for Cisco IOS XE SD-WAN devices and establishes control and data plane access in your WAN.

The Quick Connect workflow is a process in SD-WAN Manager that:

- creates a basic day-0 configuration profile for all Cisco IOS XE Catalyst SD-WAN device, regardless of device family or model,
- establish control plane (and data plane) connectivity to your WAN, and
- assigns system IP to newly onboarded devices.

Before starting the Quick Connect workflow, you must know about different methods for uploading devices for onboarding and assignment of System IP.

Device upload methods

The behavior of the Quick Connect workflow depends on how devices are uploaded to SD-WAN Manager. You can upload devices as part of the workflow or independently.

Devices can be uploaded to SD-WAN Manager in the following ways:

- Using the auto sync option, where your Smart Account is synced with SD-WAN Manager . This option requires SD-WAN Manager 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 SD-WAN Manager.

For more information on auto sync option or manual upload method, refer to these sections *Auto Sync for uploading device* and *Upload devices manually to SD-WAN Manager* that follow.

System IP address assignment

The Quick Connect workflow assigns system IP addresses to newly onboarded devices in one of these ways:

- Addresses are assigned from the system IP pool if:
  - You have defined a system IP pool (see Create a system IP pool).
  - System IP selection is set to Auto in the Quick Connect workflow.
- Otherwise, IP addresses are entered manually during the **Add and Review Device Configuration** workflow step.

Prerequisites for using the Quick Connect Workflow

This topic explains the prerequisites and configuration steps that you must perform before you use Quick Connect.

Here are the prerequisites and configuration steps that you must perform before you use Quick Connect.

- Configure the organization name.
- Configure the certificate authorization for the Cisco SD-WAN Validator and the Cisco SD-WAN Controller.
- Install and configure the controllers (Cisco SD-WAN Manager , Cisco SD-WAN Validator , and Cisco SD-WAN Controller).

> **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 the Quick Connect Workflow

Use these guidelines when configuring the Quick Connect workflow to understand its limitations, supported platforms, and device count restrictions.
WAN settings

The Quick Connect workflow is limited to configuring WAN settings (VPN 0). To complete the Cisco Catalyst SD-WAN overlay bring up process, you must also configure service-side VPN templates.

For detailed information about configuring network interfaces, refer to 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.

Run the Quick Connect Workflow

Learn how to access the Quick Connect Workflow from the SD-WAN Manager menu to start or resume device onboarding.

This procedure describes how to access the Quick Connect workflow from the SD-WAN Manager menu, including options to start a new workflow or resume an in-progress one.

1. From the SD-WAN Manager menu, choose **Workflows**.
2. Do one of these based on your stage in the workflow.
   - Start a new Quick Connect workflow: Under the **Library** area, choose **Quick Connect** and follow the onscreen instructions.
   - Resume an in-progress Quick Connect workflow: Under the **In-progress** area, click **Quick Connect** and continue to follow the onscreen instructions for next steps.

   > **Note**
   >
   > If you upload devices to SD-WAN Manager using the manual upload method, 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, refer to On-Site Bootstrap Process for Cisco SD-WAN Devices.

3. In the **Sync your device inventory** step,
   - **Log in your Smart Account**: When you have a Smart Account.
   - **Upload file with serial number**: When SD-WAN Manager is unable to reach the Smart Account server. Upload the file with authorized serial number list on SD-WAN Manager.
   - **Skip for now**: When your devices are already synchronized.
4. In the **Select devices to bring up** step, select the devices you want to onboard.

   From SD-WAN Manager 20.18.2, a **Skip configuration** button has been added to the Quick Connect workflow. This enhancement allows you to directly onboard a device without entering information such as **Hostname**, **System-IP**, or **Site Name**.
5. From SD-WAN Manager 20.18.2, in the **Add and Review Device Configuration** step, choose an existing **Site Name** (known as Site ID in previous versions) in the Site column or create a new one and add the **System IP**. When exporting or importing CSV files, specify the Site Name instead of Site ID, in the Site column.
6. (Optional)In the **Tag devices** step, add a tag to the device.
7. To onboard the device or devices, click **Onboard**.

Auto Sync for uploading devices

This topic explains how Quick Connect behaves when you upload devices using auto sync, including registration and synchronization requirements for Plug-and-Play services in single-tenant environments.

The auto sync method allows devices added to the Cisco Plug-and-Play (PnP) portal to be automatically synchronized to SD-WAN Manager after authenticating the Plug-and-Play service.

- Tenants in a single-tenant environment must register the Plug-and-Play service using Smart Account or Virtual Account credentials.
- Devices added to the Cisco PnP portal are auto-synced to SD-WAN Manager after authentication.
- The auto sync method supports both cloud and on-premises controller deployments, provided SD-WAN Manager can connect to the PnP portal.

Auto sync device upload

Auto sync enables seamless device onboarding by leveraging the Cisco Plug-and-Play portal and SD-WAN Manager integration.

For example, after registering the Plug-and-Play service with your Smart Account credentials, any device you add to the Cisco PnP portal is automatically synchronized to SD-WAN Manager, streamlining the onboarding process for both cloud and on-premises controllers.

Auto Sync with Cisco PnP, SD-WAN Manager 20.18.1 and earlier

After the Cisco team has configured and deployed the Cisco SD-WAN Controller s, 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, refer these reference documentation:
>
> - Cisco Plug and Play Support Guide for Cisco SD-WAN Products
> - Plug n Play Onboarding Workflow

Auto Sync with ZTP

This section describes the Quick Connect behavior when you upload devices using auto sync.

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 .

Ensure you prepare the routers for ZTP to join the overlay network automatically, refer to *Prepare Routers for ZTP* section.

1. For ZTP, unbox the device, connect its WAN port to the network.

   > **Note**
   >
   > For more information about configuring the vEdge routers to join the overlay network automatically, see Prepare Routers for ZTP .

2. Ensure that the IP settings from DHCP are configured, including 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.

Upload devices for onboarding with Auto Sync

This topic explains the process and behavior of uploading devices using the Auto Sync option, including how devices appear in the dashboard after onboarding.

The section provides information about Quick Connect behavior after you upload devices using auto sync.

Onboard devices using Auto Sync

After onboarding devices using the Auto Sync, you can access SD-WAN Manager dashboard using one of these methods based on the SD-WAN Manager version.

- If you upload devices to 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 SD-WAN Manager dashboard. To access the dashboard, navigate to **Monitor** > **Overview** .
- Cisco vManage Release 20.6.1 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 SD-WAN Manager dashboard. To access the dashboard, navigate to **Dashboard** > **Main Dashboard** .

Upload devices manually to SD-WAN Manager

Upload devices manually to SD-WAN Manager.

You can choose to upload your devices to SD-WAN Manager manually, if:

- You don't want to use the auto sync option, which requires you to sync your Smart Account with SD-WAN Manager.
- Your SD-WAN Manager instance is unable to connect with the Cisco PnP portal.

Upload devices to SD-WAN Manager manually

Provides steps for manually uploading devices to SD-WAN Manager.

Refer to the *Prerequisites for Using the Quick Connect Workflow* section.

Follow this procedure to manually upload your devices to 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 to **Control Components**.

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

Learn about the Quick Connect behavior with manual upload of devices.

If you upload your devices to SD-WAN Manager using the manual method, they do not appear in the 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 IOS XE Catalyst SD-WAN devices using the CLI bootstrap configuration, see On-Site Bootstrap Process for Cisco SD-WAN Devices.

10 Installing Cisco SD-WAN Control Components in the AWS Cloud

Topics:

- Feature history for installing Cisco SD-WAN Control Components in the AWS Cloud
- Installing Cisco SD-WAN Control Components in AWS
- Prerequisites for SD-WAN Control Components deployment in AWS
- Use cases for SD-WAN Control Component deployment in AWS
- Installing Cisco SD-WAN Control Components in AWS
- Install SD-WAN Control Components in AWS
- Verify the deployment of SD-WAN Control Component s in AWS
- Monitor the deployment of SD-WAN Control Component in AWS

Feature history for installing Cisco SD-WAN Control Components in the AWS Cloud

Lists the development milestones and release information for how to deploy SD-WAN Control Components in the Amazon Web Services (AWS) cloud, including feature description.

This table describes the developments of this feature, by release.

Table 28: Feature History

Feature Name	Release Information	Description
Install Cisco SD-WAN Control Components in AWS	Cisco vManage Release 20.6.1	This feature enables you to install the SD-WAN Control Components (SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator) in an AWS environment.

Installing Cisco SD-WAN Control Components in AWS

This topic explains how to deploy SD-WAN Control Components in AWS, including supported images, deployment considerations, and support guidelines for Cisco SD-WAN controllers in the Amazon Web Services environment.

The SD-WAN Control Components are parts of the SD-WAN fabric that consist of SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator. These components are installed in an Amazon Web Services (AWS) environment using Amazon Machine Images (AMI).

We provide AMI for installing SD-WAN Control Components only for you. Do not share them with others.

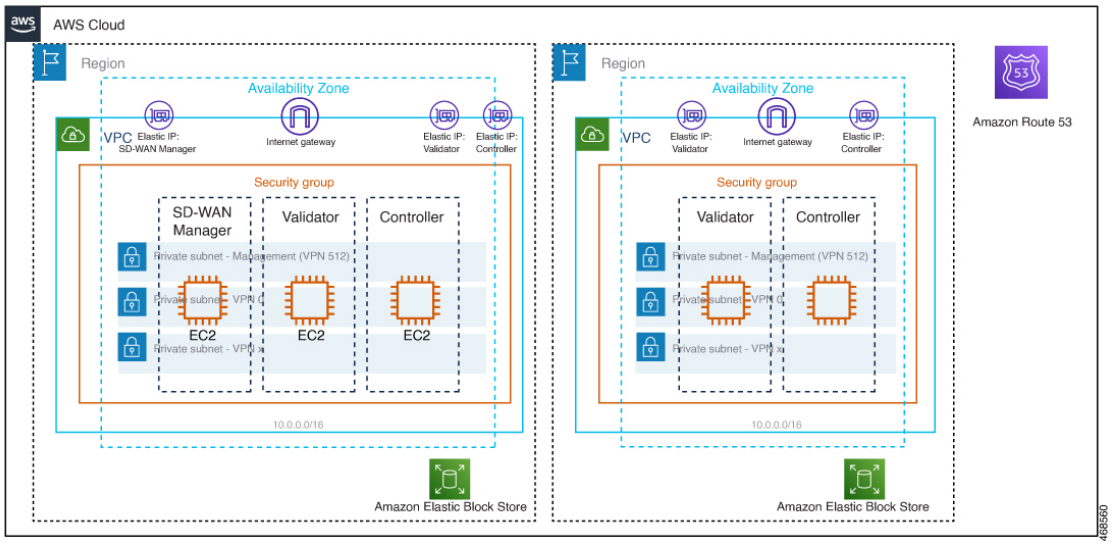
Considerations before installing SD-WAN Control Components in AWS

Before installing SD-WAN Control Components in AWS, review these considerations and support guidelines:

- Ensure minimum controller image versions are Cisco SD-WAN Manager Release 20.6.1, Cisco Controller Release 20.6.1, and Cisco Validator Release 20.6.1.
- Cisco Catalyst SD-WAN controller AMIs are not available on the Cisco software download site or AWS marketplace. They are provided only upon request with a valid business case to set up SD-WAN Control Components in your AWS cloud account.
- For information about ordering SD-WAN Control Components to use with AWS, contact your Cisco account team or Cisco partner.
- We do not provide support for any issues that arise with the cloud infrastructure during the provisioning or installation of the controllers.
- Troubleshooting:
  - Functionality issues: 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 does not 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* .

The illustration below shows the architecture of the AWS region, virtual private cloud (VPC), security group, and so on, and it shows where the SD-WAN Control Components function within the architecture.

Figure 3: SD-WAN Control Components in AWS



When you order the customer hosted deployment option of SD-WAN Control Components, ensure you included all types of control components you need for your SD-WAN deployment (SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator). The Cisco Cloud Infrastructure team only shares the AMI(s) for your ordered control component(s).

After you receive the AMI(s), you can copy or move between regions and different AWS accounts that you own. After the initial deployment of SD-WAN Control Components, you are responsible for managing all subsequent upgrades or downgrades.

Benefits of deploying SD-WAN Control Components 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 SD-WAN Control Components deployment in AWS

Outlines prerequisite requirements for deploying SD-WAN Control Components in AWS, covering supported software, account setup, infrastructure assets, and key dependencies for a successful installation.

- 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 SD-WAN Control Component deployment in AWS

Describes common use cases and deployment scenarios for Cisco SD-WAN Control Components in AWS, demonstrating practical benefits and applications for various network environments.

This section provides use cases for deploying SD-WAN Control Components in AWS to help you determine suitable scenarios for implementation.

- Use case 1: For complete control of provisioning, management and monitoring of SD-WAN Control Components and scalability using your own public cloud account.
- Use case 2: For specific architectural or security posture requirements.

Installing Cisco SD-WAN Control Components in AWS

This topic explains how to deploy SD-WAN Control Components in AWS, including supported images, deployment considerations, and support guidelines for Cisco SD-WAN controllers in the Amazon Web Services environment.

The SD-WAN Control Components are parts of the SD-WAN fabric that consist of SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator. These components are installed in an Amazon Web Services (AWS) environment using Amazon Machine Images (AMI).

We provide AMI for installing SD-WAN Control Components only for you. Do not share them with others.

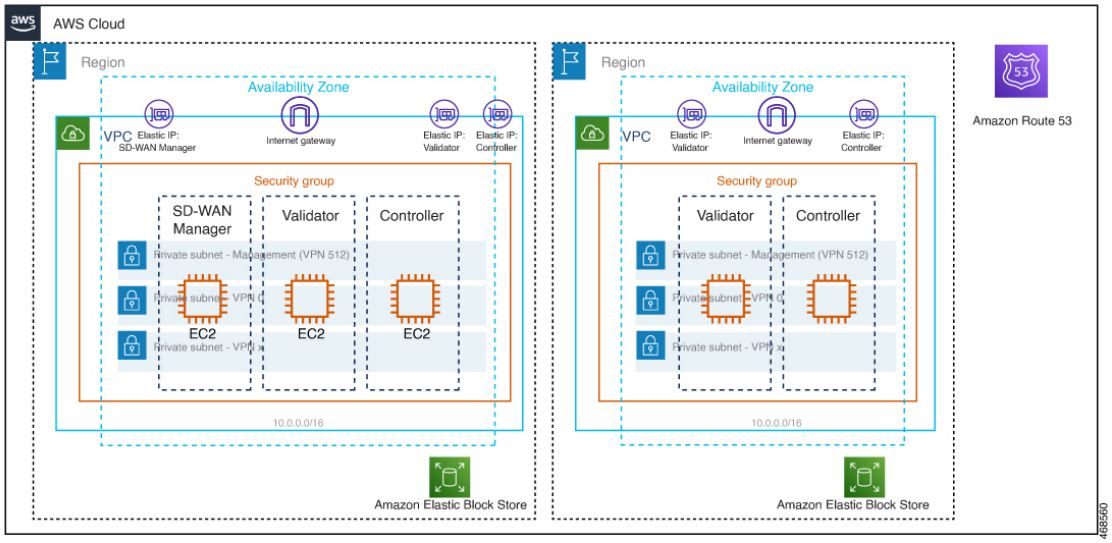
Considerations before installing SD-WAN Control Components in AWS

Before installing SD-WAN Control Components in AWS, review these considerations and support guidelines:

- Ensure minimum controller image versions are Cisco SD-WAN Manager Release 20.6.1, Cisco Controller Release 20.6.1, and Cisco Validator Release 20.6.1.
- Cisco Catalyst SD-WAN controller AMIs are not available on the Cisco software download site or AWS marketplace. They are provided only upon request with a valid business case to set up SD-WAN Control Components in your AWS cloud account.
- For information about ordering SD-WAN Control Components to use with AWS, contact your Cisco account team or Cisco partner.
- We do not provide support for any issues that arise with the cloud infrastructure during the provisioning or installation of the controllers.
- Troubleshooting:
  - Functionality issues: 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 does not 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* .

The illustration below shows the architecture of the AWS region, virtual private cloud (VPC), security group, and so on, and it shows where the SD-WAN Control Components function within the architecture.

Figure 4: SD-WAN Control Components in AWS



When you order the customer hosted deployment option of SD-WAN Control Components, ensure you included all types of control components you need for your SD-WAN deployment (SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator). The Cisco Cloud Infrastructure team only shares the AMI(s) for your ordered control component(s).

After you receive the AMI(s), you can copy or move between regions and different AWS accounts that you own. After the initial deployment of SD-WAN Control Components, you are responsible for managing all subsequent upgrades or downgrades.

Benefits of deploying SD-WAN Control Components 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.

Install SD-WAN Control Components in AWS

Guides users through the installation process for SD-WAN Control Components in AWS, including requesting AWS AMI images, creating virtual networks and subnets, deploying virtual machines, and configuring security groups to enable secure connectivity.

The procedures described here are the stages in installing the SD-WAN Control Components in AWS.

- Task 1: Request AWS AMI images on page 130.
- Task 2: Create a virtual network, subnets, and network security group in AWS on page 130
- Task 3: Create a virtual machine for the SD-WAN Control Components on page 131
- Task 4: Configure the Security Group on page 133

Request AWS AMI images

This topic describes how to deploy SD-WAN Control Components in an AWS account using AMI images.

1. You must place an order for $0 customer managed SD-WAN Control Component SKU. For more information, refer to the Catalyst SD-WAN Control Component 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 reaches out to you asking for additional details such as:
   a) AWS account number.
   b) Software version requirement for the AMI.
3. The 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, we reserve the right to remove the images and take any necessary action to prevent the images from being shared.

Create a VPC, Subnet, and Security Group in AWS.

Create a virtual network, subnets, and network security group in AWS

This topic describes how to create a VPC, Subnet, and Security Group in AWS.

> **Note**
>
> For definitive information about tasks in AWS, see the AWS documentation.

Follow these steps to create virtual network, subnets, and network security group in AWS.

1. Create a virtual private cloud (VPC), and while creating the VPC ensure that you complete these actions:
   a) Enter a name and a region for the VPC.
   b) Enter an address space for the VPC (for example, 10.0.0.0/16).
   c) Add a minimum of two subnets to the VPC, and an additional subnet if you plan to create a 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 subnets:
      - Add subnet 0 with the address 10.0.1.0/24, which will be used by VPN 512 as the primary interface for the SD-WAN Control Components.
      - Add subnet 1 with the address 10.0.2.0/24, to use it as the controllers' transport or tunnel interface for VPN 0.
      - Add subnet 2 with the address 10.0.3.0/24, to use it for SD-WAN Manager clustering (this is only required when deploying a SD-WAN Manager cluster).
   d) (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.

a) The security group must contain these:
   - 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 for each controller to reach other controllers.

b) Enter a name and a region for the security group.
c) (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.

Create a virtual machine for the SD-WAN Control Components.

Create a virtual machine for the SD-WAN Control Components

This topic describes how to create a virtual machine for the SD-WAN Control Component.

> **Note**
>
> For definitive information about tasks in AWS, see the AWS documentation.

Follow these steps to create a virtual machine for the SD-WAN Control Component.

1. Begin the workflow for creating a virtual machine. When creating a virtual machine, ensure that you complete these steps:
   a) Install the virtual machine in the virtual private cloud (VPC) created in task "Create a VPC, Subnet, and Security Group in AWS".
   b) Enter a name and region for the virtual machine.
   c) 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.

   d) 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.
   e) For disk resources, perform one of these options:
   - If you are deploying a SD-WAN Controller or a SD-WAN Validator, no additional disk resources are required beyond the default.
   - If you are deploying a SD-WAN Manager, choose one additional disk.
     - Choose the Premium SSD option and default encryption.
     - Choose a disk size of 1 TB (General Purpose SSD gp3) or larger.

For server recommendations relevant to controllers in AWS, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

- 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.
- For Cisco SD-WAN Controller Release 20.6.1 and later, you have an option to use the user 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 that you created in an earlier task.

- If you are deploying a SD-WAN Controller or a SD-WAN Validator, create one additional network interface.
- If you are deploying a SD-WAN Manager, create two additional network interfaces.
- If you are deploying a SD-WAN Manager in a cluster, see Cluster Management and Deploy Cisco SD-WAN Manager for additional information about SD-WAN Manager out-of-band interfaces.

3. When creating a network interface, complete these 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 SD-WAN Manager controller, associate NIC 2 with subnet 2.
  - If you are using a 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 Elastic IP in AWS.

5. When creating a public IP, ensure that you complete the following actions:

   - For assignment, choose static.
   - To specify NIC 1, use the associate option.

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 SD-WAN Controller or a SD-WAN Validator, attach the NIC to the virtual machine.
   - If you are deploying 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.

Configure the Security Group.

Configure the Security Group

This topic describes how to configure the Security Group.

> **Note**
>
> For definitive information about tasks in AWS, see the AWS documentation.

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.

Follow these steps to 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 SD-WAN Control Components. If the controllers lack connectivity to each other, the control plane and the data plane cannot operate.
   - Accessing the SD-WAN Control Component 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 SD-WAN Control Components. When creating a new inbound security rule, ensure that you complete the following actions:
   a) Specify IP ranges, protocol, and so on.
   b) 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 SD-WAN Manager.

Verify the deployment of SD-WAN Control Components in AWS.

Verify the deployment of SD-WAN Control Component s in AWS

Provides instructions for validating the deployment of SD-WAN Control Components in AWS, ensuring all components operate as expected and the cloud installation is functional.

This topic describes how to verify the deployment of SD-WAN Control Components in AWS.

Infrastructure: To verify the deployment of SD-WAN Control Components in AWS, use the AWS portal to confirm that the virtual machines hosting each SD-WAN Control Component are active.

Services: To verify that Cisco Catalyst SD-WAN services are operating after deployment of the SD-WAN Control Components, follow these 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 SD-WAN Manager, and use the **request nms all status** command. The output shows the status of all the 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 SD-WAN Control Components, follow the steps in Cisco SD-WAN Overlay Network Bring-Up Process to establish the control connections for the SD-WAN Control Components and to verify that each SD-WAN Control Component is operational.

Monitor the deployment of SD-WAN Control Component in AWS

Explains how to monitor deployed SD-WAN Control Components in AWS, including procedures for ongoing health checks and performance evaluation to maintain operational reliability.

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, refer to the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

11 Deploying SD-WAN Control Components in Microsoft Azure

Topics:

- Deploy SD-WAN Control Components in Microsoft Azure
- Scenarios for SD-WAN Control Component deployments in Azure
- Deploy an SD-WAN Control Component image in Azure
- Create an SD-WAN Control Component image in Azure
- Create a Virtual Network, Subnets, and Network Security Group in Azure
- Create a virtual machine for the SD-WAN Control Component
- Configure the Network Security Group
- Verify the deployment of SD-WAN Control Components in Azure
- Monitor the deployment of SD-WAN Control Components in Azure

Deploy SD-WAN Control Components in Microsoft Azure

Outlines the deployment of SD-WAN control components–including manager, controller, and validator–in Microsoft Azure, highlights minimum image requirements, illustrates Azure integration architecture, and details benefits such as cost savings, simplified management, stability, security, and scalability.

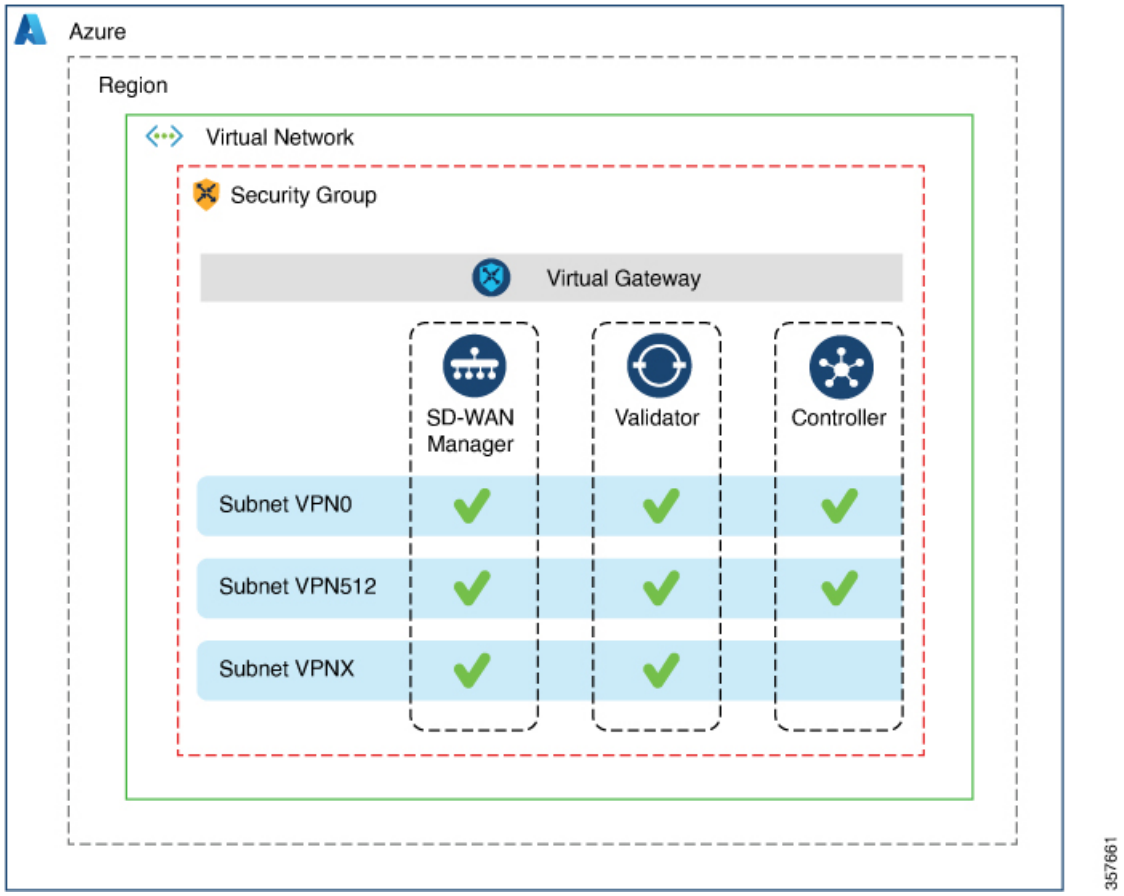
You can deploy the following SD-WAN Control Components in an Azure environment:

- SD-WAN Manager
- SD-WAN Controller
- SD-WAN Validator

The minimum supported SD-WAN Control Component image for deployment is Cisco Catalyst SD-WAN Control Components Release 20.6.1.

The following illustration shows the architecture of the Azure region, virtual network, security group, and so on, and it shows where is the function of SD-WAN Control Component within the architecture:

Figure 5: SD-WAN Control Components in Azure



Benefits of deploying SD-WAN Control Components 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 SD-WAN Control Components.
- Security: Azure provides a secure hosting environment.
- Scaling: Azure provides an easy path to increase the scale of your Cisco Catalyst SD-WAN network.

Scenarios for SD-WAN Control Component deployments in Azure

Outlines deployment scenarios for hosting control components in Microsoft Azure within Cisco Catalyst SD-WAN environments, emphasizing consistent service alignment and operational efficiency.

If your Cisco Catalyst SD-WAN deployment already uses Microsoft Azure, such as for Cisco Catalyst 8000V Edge software, you can host SD-WAN Control Components in Azure. This approach ensures consistent service alignment and operational efficiency.

Deploy an SD-WAN Control Component image in Azure

Provides step-by-step instructions for deploying control component images in Azure, including creating images, configuring virtual networks and security groups, setting up virtual machines, and enabling or disabling IPv6 ULA address handling for different component types.

The procedures described here apply to the three types of SD-WAN Control Components– SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator. Where applicable, we indicate where the instructions are different for specific components.

> **Note**
>
> In DHCP configurations, IPv6 Unique Local Addresses (ULA) are assigned to the interface in some instances. 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.

Follow these steps to deploy an SD-WAN Control Component Image in Azure.

1. Task 1: Create an SD-WAN Control Component Image in Azure
2. Task 2: Create a Virtual Network, Subnets, and Network Security Group in Azure
3. Task 3: Create a Virtual Machine for the SD-WAN Control Component
4. Task 4: Configure the Network Security Group

Create an SD-WAN Control Component image in Azure

Guides you through creating a control component image in Azure, including downloading and decompressing images, configuring storage accounts and containers, uploading VHD files, setting image properties, and establishing virtual networks, subnets, and security groups.

This procedure describes how to create an SD-WAN Control Component image in Azure.

On the Cisco Software Download page, download the images for each SD-WAN Control Component: SD-WAN Manager, SD-WAN Controller, and SD-WAN Validator. Decompress the downloaded files, which are in .tar format. The image file for each SD-WAN Control Component is in virtual hard disk (VHD) format.

Follow these steps to create an SD-WAN Control Component image in Azure.

For more information about tasks in Azure, see the Azure documentation.

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 SD-WAN Control Component.

   Note

   Each SD-WAN Control Component requires a separate container.

3. Upload the VHD file of the SD-WAN Control Component into the container.
   a) 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.

Create a virtual network, subnets, and network security group in Azure.

Create a Virtual Network, Subnets, and Network Security Group in Azure

Provides instructions for creating a virtual network, configuring subnets, establishing a network security group, and associating these resources within the Azure portal to support control component deployment.

This procedure describes how to create a virtual network, subnets, and network security group in Azure.

> **Note**
>
> For definitive information about tasks in Azure, see the Azure documentation.

Follow these steps to create a Virtual Network, Subnets, and Network Security Group in the Azure portal:

1. Begin the workflow for creating a virtual network. When creating a virtual network, ensure that you complete these activities:
   - 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 SD-WAN Catalyst 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 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 these activities:
   - 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.

Create a Virtual Machine for the control components.

Create a virtual machine for the SD-WAN Control Component

Provides step-by-step instructions for creating a virtual machine for the SD-WAN Control Component, configuring VM settings, selecting disk and network resources, setting up public IP addresses, managing network interfaces, and preparing post-deployment networking requirements in Azure.

This procedure describes how to create a virtual machine for the SD-WAN Control Component.

When creating a VM, ensure that you complete the following actions:

Follow the steps to create a Virtual Machine for the SD-WAN Control Component.

> **Note**
>
> For more information about tasks in Azure, see the Azure documentation.

1. Begin the workflow for creating a virtual machine (VM).

   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 SD-WAN Control Component 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 SD-WAN Control Component.

     For information about SD-WAN Control Component-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 an SD-WAN Controller or an SD-WAN Validator, no additional disk resources are required beyond the default.
     - If you are deploying an SD-WAN Manager component, 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 SD-WAN Control Components 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 SD-WAN Control Components.

    - Optional:
        - You can enable advanced boot diagnostics (a management option) to create an additional storage account in the resource group for storing diagnostics logs.
        - (Cisco Catalyst SD-WAN Control Component release 20.6.1) 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 SD-WAN Control Component.

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 an SD-WAN Control Component or SD-WAN Validator, create one additional network interface.
    - If you are deploying an SD-WAN Manager controller, create two additional network interfaces.
    - If you are deploying an SD-WAN Manager controller in a cluster, see Cluster Management and Deploy Cisco Catalyst SD-WAN Manager for additional information about 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 primary network interface with subnet 1.

      If you are deploying an SD-WAN Manager controller, associate secondary network interface with subnet 2.

      If you are using an SD-WAN Manager cluster, associate tertiary network interface with subnet 3.

      > **Note**
      >
      > Associating a network interface with a subnet enables the VM to connect to the subnet.

    - For each network interface, 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 primary network interface.

> **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 primary network interface.

4. Stop the VM, and confirm when it has stopped.
5. Attach the newly created network interfaces to the VM.
   - If you are deploying an SD-WAN Controller or an SD-WAN Validator, attach the network interface to the VM.
   - If you are deploying an SD-WAN Manager, attach both of the newly created network interfaces to the VM.
6. Restart the VM.

   Confirm in the Azure portal that the VM has restarted.

Configure the network security group.

Configure the Network Security Group

Provides instructions for configuring an NSG in Azure, including adding inbound security rules for controller connectivity and access, specifying rule parameters, and verifying VM connectivity and deployment.

This procedure describes how to configure the NSG in Azure.

> **Note**
>
> For more information about tasks in Azure, see the Azure documentation.

The NSG is a functionally related 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.

Follow the steps to configure the NSG.

1. Using the Azure portal, add inbound security rules to the NSG created in an earlier task. This allows inbound traffic from the IP ranges for:
   - Establishing control connections between each of the SD-WAN Control Components. If the components 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. These rules must allow all the controller VM IP addresses, to enable the required connectivity between the SD-WAN Control Components.

   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 primary network interface with the public IP of SD-WAN Manager.

Verify the deployment of SD-WAN Control Components in Azure.

Verify the deployment of SD-WAN Control Components in Azure

Outlines procedures for verifying deployment and operation of control components in Azure, including checking VM activity, confirming SD-WAN services status, and establishing control connections for SD-WAN Control Components.

This procedure describes how to verify deployment of SD-WAN Control Components in Azure.

> **Note**
>
> For more information about tasks in Azure, see the Azure documentation.

- Infrastructure: To verify the deployment of SD-WAN Control Components within virtual machines in Azure, use the Azure portal to check that the VMs hosting each SD-WAN Control Component are active.
- Services: The procedure in next section describes the procedure to verify that Cisco Catalyst SD-WAN services are operating after deployment of the SD-WAN Control Components.

Follow these steps to verify Cisco Catalyst SD-WAN services.

1. Check for a successful ping to the VM that hosts SD-WAN Manager.
2. Log in to SD-WAN Manager.
3. Use SSH to connect to SD-WAN Manager, and use the **request nms all status** command. The output shows the status of all of the SD-WAN Manager services. Ensure 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 theSD-WAN Control Components, follow the steps in Cisco SD-WAN Overlay Network Bring-Up Process to establish the control connections for the SD-WAN Control Components and to verify that each controller is operational.

Monitor the deployment of SD-WAN Control Components in Azure

Guides you through monitoring infrastructure status, including CPU and disk usage, using Azure portal tools, and directs you to resources for monitoring SD-WAN service health.

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.

12 Device Software Installation, Cisco IOS XE 17.2.1r and Later

Topics:

- Feature history for device software installation
- Platform support
- Cisco IOS XE image compatibility
- Self-signed trustpoint
- Autonomous and controller modes
- Restrictions for installing and upgrading device software
- Software Installation for Cisco IOS XE Routers
- Plug and Play onboarding
- Plug and Play onboarding workflow
- Non-Plug and Play onboarding
- Mode discovery and mode change with a bootstrap file
- Reset a device to a Controller mode day zero configuration using CLI commands
- Configuration persistence during mode switch
- Verifying Controller and Autonomous modes
- Change the console port access after installation, in Controller mode
- Restoring Smart Licensing after switching modes

Information about device software installation.

Feature history for device software installation

History of features that relate to installing and upgrading the software of network devices.

This table describes the history of features that relate to installing software on network devices.

Table 29: 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.
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.
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.

Platform support

Describes the platforms that support the installation and upgrade procedures described here.

Describes the platforms that support the installation and upgrade procedures described here.

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)
- 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

Which software image types to use for platforms operating in Cisco Catalyst SD-WAN.

Describes which software image types to use for platforms operating in Cisco Catalyst SD-WAN.

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).

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.

Describes the self-signed trustpoint that is generated and loaded to a device when it boots up.

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.

Autonomous and controller modes

Two installation modes are available.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.

Describes the two installation modes that are available on devices. Autonomous mode supports the functionality of Cisco IOS XE in a non-Cisco Catalyst SD-WAN deployment and Controller mode supports the Cisco Catalyst SD-WAN solution.

Table 30: Comparison of modes

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)
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

Restrictions for installing and upgrading device software

Restrictions relevant for installing and upgrading software on devices in a Cisco Catalyst SD-WAN environment.

Describes restrictions relevant for installing and upgrading software on devices in a Cisco Catalyst SD-WAN environment.

Dual-IOSd

Dual-IOSd is supported only in autonomous mode.

Requirement of universalk9 images

Software 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.

Changing mode clears configuration

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

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, the WebUI is not supported, and an error message is displayed if used.

Keep existing image

When upgrading, do not delete the existing image. This provides a software rollback option.

If upgrade fails

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.

Upgrading a device to to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

When upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from Cisco IOS XE Releases 17.3.1a or earlier, do not make any changes to the device configuration using CLI commands 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 commands, the device can have inconsistent configuration and the upgrade fails. If you perform the upgrade 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, upgrade the device using Cisco Catalyst SD-WAN.

Firmware upgrade: primary and backup tunnel interfaces

From 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, refer to the **vmanage-connection-preference** command in the *Cisco Catalyst SD-WAN Command Reference Guide*. Configuring an interface with a higher preference value gives the interface a higher priority.

Downgrading devices to releases earlier than 17.1.x

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.

Software Installation for Cisco IOS XE Routers

Software installation for different platforms, in the context of Cisco Catalyst SD-WAN.

Describes software installation for different platforms, in the context of Cisco Catalyst SD-WAN.

Software image type

Software image type to download.

Describes the software image type to download.

For devices operating with Cisco Catalyst SD-WAN, the software image to use has a filename in this pattern:

<router-model>-universalk9.<release-number>

Images are available on the Cisco Software Download site.

Installing software on select platforms

Provides links to documents for information about installing software on specific platforms.

Provides links to documents for information about installing software on specific platforms.

Refer to these documents for installation instructions:

- 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 the Cisco Catalyst 8000V Edge Software platform

Information about installing software on the Cisco Catalyst 8000V Edge software platform.

Provides information about installing software on the Cisco Catalyst 8000V Edge software platform.

From 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.

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*.

Software image

Use 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

Controller mode

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.

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.

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.

Install software on the Cisco CSR 1000v platform

Links to detailed information about installing software on the Cisco CSR 1000v platform.

Provides links to detailed information about installing software on the Cisco CSR 1000v platform.

Based on the cloud service in which you are deploying the CSR 1000v instance, see this information about performing the bootstrap or the day 0 configurations:

- 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

Plug and Play onboarding

Information about onboarding devices through Cisco Plug and Play.

Provides information about onboarding devices through Cisco Plug and Play.

Plug and Play onboarding workflow

Steps for onboarding devices to Cisco Catalyst SD-WAN using Plug and Play.

Note these considerations regarding Plug and Play:

- 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.

- 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.

For more information, refer to the Plug and Play Support Guide.

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.

Mode discovery with Plug and Play onboarding

The PnP-based discovery process determines the mode in which the device operates, and initiates a mode change if required.

Describes how the Plug and Play (PnP)-based discovery process determines the mode and changes it if necessary.

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change if necessary. The mode change causes the device to reboot. After the reboot, the device performs the appropriate discovery process.

When you upgrade to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, on a Cisco device running an earlier verion of Cisco IOS XE or a Cisco Catalyst SD-WAN image, the device starts in Autonomous mode or Controller mode depending on the configured controller.

Deployment using Plug and Play (PnP) may include any of these discovery process scenarios:

Table 31: PnP discovery process scenarios

Bootup 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

Bootup mode	Deployment mode	On-boarding agent	Cisco SD-WAN Validator	Discovery process	Mode change
Controller	Cisco SD-WAN Manager	Plug and Play	Yes	Plug and Play Connect Discovery	No mode change

Automatic IP address detection

Describes how a device can automatically learn about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets.

Describes how a device can automatically learn about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets.

How a device receives IP address and gateway server information during PnP onboarding

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.

Automatic IP address detection applies only to day zero deployments and is enabled by default.

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.

IP address not preserved after reboot

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.

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.

Restrictions for automatic IP address detection

- Automatic IP address detection 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.
- Automatic IP address detection is supported only on devices that are in Controller mode, for configuration by Cisco Catalyst SD-WAN.
- Automatic IP address detection 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.

- Automatic IP address detection 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-Plug and Play onboarding

How to onboard devices to Cisco Catalyst SD-WAN without using Plug and Play (PnP).

Describes how to onboard devices to Cisco Catalyst SD-WAN without using Plug and Play (PnP).

New installation: Mode change device day zero scenario

A prerequisite for this process is a bootstrap file.

For software devices such as Cisco Catalyst 8000V Edge Software, 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.

Describes the process by which a new device determines which mode to use (Autonomous or Controller) and boots up.

1. If a 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 device determines if a mode change is required, based on the bootstrap file, and boots up.
   - If the ciscosdwan.cfg or ciscosdwan_cloud_init.cfg bootstrap files are available 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.

     The bootstrap file (ciscosdwan.cfg) is generated by Cisco SD-WAN Manager, and has a UUID, but no OTP.
   - If a ciscortr.cfg bootstrap file or config-wizard is discovered, mode change is not initiated and the boot up continues in Autonomous mode.

Change a device to Autonomous mode

Procedure for changing a device to Autonomous mode.

Use the **controller-mode disable** command only to temporarily change the device to Autonomous mode. Return the device to Controller mode using the same image.

> **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.

1. Use the **controller-mode reset** command to take the device back to the day zero configuration.

```
Device# controller-mode reset
```

2. Use the **controller-mode disable** command to switch the device to Autonomous mode.

```
Device# controller-mode disable
```

Change a device to Controller mode

Procedure for changing 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.

> **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.

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.
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. Verify that the device expanded the image file.

Viewing the sdwaninstaller directory

Conditions in which you cannot view the contents of the sdwaninstaller directory.

Describes conditions in which you cannot view the contents of the sdwaninstaller directory.

You cannot view the contents of the bootflash:/.sdwaninstaller directory or .sdwanistallerfs file of a Cisco IOS XE Catalyst SD-WAN device in either of these 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 possible when the file and directory are hidden.

Mode discovery and mode change with a bootstrap file

Explains mode discovery and mode change with a bootstrap file.

Describes mode discovery and mode change using a bootstrap file.

Preventing a device from booting in Controller mode

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 Controller mode. To prevent the device from booting up in Controller mode, before performing the device upgrade, ensure that you remove the stale Cisco Catalyst SD-WAN configuration file from the bootflash, and delete all artifacts of Cisco Catalyst SD-WAN from the bootflash.

To delete all the artifacts:

- 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

Configuration file prerequisites for mode change

Table 32: Configuration file prerequisites

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

Upgrading a device already running a Cisco Catalyst SD-WAN image

On a device that is already running 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.

Booting Cisco CSR 1000v and Cisco Catalyst 8000V devices in Controller mode

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

Reset a device to a Controller mode day zero configuration using CLI commands

Describes how to reset a device to a Controller mode day zero configuration using a CLI command.

Erase the Cisco Catalyst SD-WAN configuration of the current active image to a reset a device to a Controller mode day zero configuration.

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 performing the configuration reset operation.

> **Note**
>
> Failure to follow save the bootstrap file in these environments causes loss of virtual machine connectivity.

1. To erase the Cisco Catalyst SD-WAN configuration of the current active image, use the **request platform software sdwan config reset** CLI command

```
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.
```

2. Reload the router after running the CLI command.

Executing this CLI command ensures the configuration for the currently installed version is wiped, together with crypto keys. The device enters the day zero workflow after the reload.

One of these occurs next:

- If the device is set up to use PnP for onboarding, then PnP discovery begins.

- 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.

Configuration persistence during mode switch

Configuration retention and erasure when switching a device between Autonomous and Controller modes.

Describes configuration retention and erasure when switching a device between Autonomous and Controller modes.

Table 33: Mode switch behavior

Current configuration mode	Switching to	Behavior
Autonomous	Controller	Erases the contents of NVRAM and the startup configuration. Device reverts to a day zero configuration. The previous running configuration is stored in bootflash. The configuration is not restored. **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 can manually restore the configuration from a backup.
Controller	Autonomous	Erases the ConfD configuration database (CDB) contents, for subsequent mode switches, and the Cisco IOS XE configuration is not restored, as the startup configuration is empty. You can manually restore the configuration from a backup.

Verifying Controller and Autonomous modes

The **show** commands to use on a device to verify Controller or Autonomous mode.

Describes the **show** commands to use on a device to verify Controller or Autonomous mode.

Verifying 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 a device is in Controller mode, the **show sdwan running-config** command does not display this 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.

Verifying 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
```

Change the console port access after installation, in Controller mode

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.

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.

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 these options to configure the type of access:
   - virtual: This option specifies that the device is accessed through the hypervisor virtual VGA console.
   - 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 **platform console serial** command to the CLI add-on profile or CLI add-on template. This helps prevent Cisco SD-WAN Manager from 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.

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
```

This step reboots the device in controller mode.

Restoring Smart Licensing after switching modes

Restoring Smart Licensing authorization lost when a device switches from Autonomous to Controller mode.

Describes methods to restore Smart Licensing authorization lost when a device switches from Autonomous to Controller mode.

When a device swtiches from Autonomous mode to Controller mode and back to Autonomous mode again, it loses authorization for Smart Licensing.

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.

Restore Smart Licensing

Procedure for enabling Smart License reservation.

1. Configure the device to reach Cisco Smart Software Manager (CSSM).
2. Register the device using the **license smart register idtoken** *token* **force** command in privileged EXEC mode.
3. Set the required crypto throughput using the **platform hardware throughput crypto** *crypto-value* command.
4. Save the configuration using the **write memory** command 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.

13 Cisco SD-AVC

Topics:

- Feature history for Cisco SD-AVC
- Cisco SD-AVC
- Cloud-hosted SD-AVC
- Installing and enabling Cisco SD-AVC, Releases 20.3.1 and later
- Enable Cisco SD-AVC on Cisco vManage Release 20.3.1 through SD-WAN Manager 20.16.x
- Enable Cisco SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices

Feature history for Cisco SD-AVC

Developments in Cisco SD-AVC, by release.

Developments in Cisco SD-AVC, by release.

Table 34: Feature history

Feature name	Release information	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

Cisco SD-AVC is a component operating within Cisco Catalyst SD-WAN that provides recognition of network application traffic, and provides analytics at the network level.

Cisco SD-AVC is a component operating within Cisco Catalyst SD-WAN that

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

Cloud-hosted SD-AVC

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.

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.

Benefits

- 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.

Environment type	Uses cloud-hosted SD-AVC	From this release	Comments
Cisco Catalyst SD-WAN Cloud (formerly Cisco Cloud-delivered Catalyst SD-WAN)	Yes	Cisco Catalyst SD-WAN Control Components Release 20.10.1	
Cisco Catalyst SD-WAN Cloud Pro (formerly Cisco Hosted Catalyst SD-WAN)	Yes	Cisco Catalyst SD-WAN Control Components Release 20.10.1	
On-premises installations of Cisco Catalyst SD-WAN where internet access is available, and where the Cloud Services feature is enabled	Yes	Cisco Catalyst SD-WAN Control Components Release 20.18.1	
Air-gapped environments without internet access	No	–	Uses a local SD-AVC service.
Environments with the Cloud Services feature not enabled	No	–	Uses a local SD-AVC service.

Restrictions for cloud-hosted SD-AVC

Restrictions for cloud-hosted SD-AVC.

Describes restrictions for cloud-hosted SD-AVC.

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.

Installing and enabling Cisco SD-AVC, Releases 20.3.1 and later

Cisco SD-AVC is pre-installed from 20.3.1 and pre-enabled from 20.18.1. Details described here.

Cisco SD-AVC is pre-installed from 20.3.1 and pre-enabled from 20.18.1. The details are described here.

Pre-installed from 20.3.1

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

Enabled by default from 20.18.1

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.

Upgrading to 20.18.1 or later

If you upgrade an environment to SD-WAN Control Components 20.18.1 or later from earlier releases, SD-AVC is not necessarily enabled. The SD-AVC status before upgrade is preserved after upgrade. For example, if you have a 20.17.x installation, with SD-AVC disabled, and you upgrade to 20.18.1, SD-AVC remains disabled. This is true even though from 20.18.1, SD-AVC component is enabled by default in new installations.

Enable or disable in **Administration** > **Settings** > **SD-AVC**.

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

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

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

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

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

Describes how to enable SD-AVC on a Cisco IOS XE Catalyst SD-WAN device.

To enable SD-AVC on a 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.

- 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.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Select **Localized Policy**.
3. To add a policy and enable Application, follow these steps:
   a) Select **Add Policy**.
   b) Click **Next** on several pages (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** page.
   c) In the **Policy Overview** page, 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 these steps:
   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) Select **Additional Templates**.
   d) Add the localized policy created in an earlier step of this procedure.
   e) Select **Update** and proceed through the next screens to push the updated template to the device.
5. 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
```

14 SD-AVC Cloud Connector

Topics:

- Feature history for Cisco SD-AVC Cloud Connector
- Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later
- Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x
- Enable Cloud Services

Feature history for Cisco SD-AVC Cloud Connector

Developments in Cisco SD-AVC Cloud Connector, by release.

Developments in Cisco SD-AVC Cloud Connector, by release.

Table 35: 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

Information about enabling 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.

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

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

Information about enabling Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x.

- 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 36: 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	**Note** 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-us-01.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-us-01.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.

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. Do one of these:
   a) If you need to enter the cloud gateway URL, use: datamanagement-us-01.sdwan.cisco.com
   b) 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.
   c) 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 these:
      - 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.

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

   Refer to the information 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.

4. (For Cisco vManage Release 20.9.x and earlier releases) Enter these 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.

.

Enable Cloud Services

Enable Cloud Services functionality.

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

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Select **Cloud Services**.
3. Enable **Cloud Services** in the **Cloud Services** tab.
4. Enter your Smart Account credentials in the fields.
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.

6. Click **Save**.

15 Cisco Services Authentication

Topics:

- Feature history of Cisco services registration
- Authentication for Cisco services
- Restrictions for authenticating Cisco services
- Authenticate Cisco services

Describes how SD-WAN Manager enables registration for multiple Cisco services using identity provider-based (IdP) authentication, providing a secure method to authenticate users and obtain access tokens without storing credentials in SD-WAN Manager.

Feature history of Cisco services registration

Outlines the feature history of Cisco services registration by release, detailing authentication developments such as identity provider-based registration and enabling users to register and authenticate multiple services simultaneously.

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

Outlines IdP-based authentication methods for Cisco services, highlighting secure user access token management and providing guidance on re-registering UTD, License, and other integrated services after upgrade.

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

Outlines recommended actions for re-authenticating Cisco services with different credentials, including clearing browser cookies, switching browsers, or using Incognito mode to avoid credential conflicts.

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

Guides you through authenticating multiple Cisco services using IdP-based authentication from the services registration page, including selecting services for different environment types, completing registration steps, and managing account credentials.

You can authenticate multiple Cisco services at once with IdP-based authentication from the Cisco services registration page.

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

4. Click **Register services**.

   A pop-up window appears with the user code.
5. Click **Next**.
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.