Hardware and Software Installation

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

Table 1: Feature History

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

- Upgrade Memory and vCPU Resources on a Virtual Machine Hosting Cisco Catalyst SD-WAN Manager, on page 45
- Use Software Maintenance Upgrade Package on Cisco IOS XE Catalyst SD-WAN Devices, on page 47

Server Recommendations

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

vEdge Cloud Router Server Recommendations

Refer to vEdge Cloud Datasheet.

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

Prerequisites

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

OIR Support

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

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

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

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

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

Reset Device Configuration

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

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

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

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

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

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

Device Requirements

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

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

Perform the On-Site Bootstrap Process

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

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

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

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

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

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

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

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

   c. Click **Manual**.

   d. Click **Save**.

4. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
5. Click **Feature Templates** and create a template for the device.

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 2: Feature History

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

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

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

How Cisco vEdge 5000 is Authenticated using OTP and Public Key

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

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

Points to Consider

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

Prerequisites

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

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

View or Add Public Key for a Cisco vEdge 5000 Device

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

The **Device Information** is displayed.

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

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

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

Bootstrap Procedure

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

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

   The WAN Edge List is uploaded to controllers.

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

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

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

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

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

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

Note

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

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

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

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

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

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

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

 HARDWARE

  INSTALLED   SUBJECT

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

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

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

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

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

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

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

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

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

9. Download CSR.

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

b. Select the Cisco vEdge 5000 device for which to sign a certificate.

c. For the selected device, click **...** and select **View Enterprise CSR**.

d. To download the CSR, click **Download**.

10. Send the certificate to a third-party signing authority and have them sign it.

11. To install the certificate on the device, perform the following steps:

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

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

b. Click **Install Certificate** button located in the upper-right corner of the screen.

c. In the **Install Certificate** screen, paste the certificate into the **Certificate Text** field, or click **Select a File** to upload the certificate in a file.

d. Click **Install**.

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

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

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

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

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

13. Remove the USB drive from the device.

Outcome

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

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

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

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

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

bootflash:/ciscosdwan.cfg

Prerequisites

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

Procedure

1. On the Cisco IOS XE Catalyst SD-WAN device, establish connectivity to Cisco SD-WAN Manager, by configuring the following:
    - System IP address
    - Domain ID
    - Site ID
    - sp-organization-name
    - organization-name
    - Cisco SD-WAN Validator IP address and port number
    - Tunnel with encapsulation configured as either GRE or IPSEC

    Example:

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

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

   Example:

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

   The configuration file is saved to this location:

   bootflash:/ciscosdwan.cfg

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

Table 3: Feature History

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

Overview of Generic Bootstrap Configuration

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

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

The generic bootstrap configuration contains the following:

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

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

How the Generic Bootstrap Configuration Works

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

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

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

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

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

   The file is named in the format `<filename>.cfg`.
5. Rename the generic bootstrap configuration file as `ciscosdwan.cfg`.
6. Copy the `ciscosdwan.cfg` file to a bootable USB drive or to the bootflash of the device.
7. If you are using a USB drive, plug the USB drive into the device.
8. Reset the device software configuration by issuing the following commands on the CLI:

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

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

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

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

     The device connects to the Cisco SD-WAN Validator and is listed as an unclaimed WAN edge device on the Cisco SD-WAN Validator and Cisco SD-WAN Manager.

- On the Cisco SD-WAN Validator, you can view the unclaimed WAN edge devices by using the command **show orchestrator unclaimed-vedges**.
- In Cisco SD-WAN Manager, you can view the unclaimed WAN edge devices by selecting **Configuration** > **Devices** > **Unclaimed WAN Edges**.

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

10. Claim the device on Cisco SD-WAN Manager:

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

a. Choose the device you wish to claim and click **Claim Device(s)**.

- The device is removed from **Unclaimed WAN Edges** and listed on **WAN Edge List**.
- On the Cisco SD-WAN Validator, the device is listed as a valid WAN edge device. You can view the valid WAN Edge devices by issuing the command **show orchestrator valid-vedges**.

11. Attach a configuration template to the device.

a. Ensure that the template includes the system IP address and the site ID.

b. Push the template to the device.

Result

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

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

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

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

1. Detach device from templates:

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

b. Click **Device Templates** and select the template attached to the device.

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

c. For the selected template, click **...** and choose **Detach Devices**.

d. In the **Available Devices** column, select the device to be detached from the template.

e. Click the arrow pointing right to move the device to the **Selected Devices** column.

f. Click **Detach**.

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

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

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

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

Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier

Note Beginning with Cisco vManage Release 20.3.1/Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the Cisco SD-AVC installation has changed. See Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later, on page 18.

Overview

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

What are the benefits of this feature?

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

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

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

The following table describes the SD-AVC installation requirements.

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

Enabling SD-AVC on Cisco SD-WAN Manager

Prerequisites

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

Procedure

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

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

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

   b. Verify that the checksum of the downloaded image matches this.
2. To upload the SD-AVC virtual service package to Cisco SD-WAN Manager:
   a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
   b. Click **Virtual Images** and select **Upload Virtual Image** to upload the SD-AVC package.

3. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** page.
4. For the desired host (the Cisco SD-WAN Manager portal on which you are enabling SD-AVC), click **…** and choose **Edit**.
5. In the Edit Cisco SD-WAN Manager dialog box, enter the username and password, using Cisco SD-WAN Manager credentials.
6. Select the checkbox for **Enable SD-AVC**. Click **Update**.
7. Cisco SD-WAN Manager prompts you to confirm before rebooting the device to apply the changes to the device. Click **OK** to confirm.
8. After the reboot, Cisco SD-WAN Manager comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.
9. (Optional) After installation is complete, you can verify that Cisco SD-WAN Manager has the SD-AVC virtual service installed and operating correctly.
   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
   b. In Service Configuration, in Cisco SD-WAN Manager row of the table, verify that the SD-AVC shows a green checkmark.

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

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

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

Prerequisites

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

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
   a. Click **Add Policy**.
   b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
   c. In the **Policy Overview** screen, enter a policy name and policy description.
   d. Select **Application**.

e. Save the policy.

4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. For the device on which you have to enable SD-AVC, click **…** and select **Edit** from the menu.
   c. Click **Additional Templates**.
   d. Add the localized policy created in an earlier step of this procedure.
   e. Click **Update** and proceed through the next screens to push the updated template to the device.
5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.

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

   or

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

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

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

For information about Cisco SD-AVC, see Cisco SD-AVC.

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

Prerequisites

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

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

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

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

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

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

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

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

Prerequisites

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

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
   a. Click **Add Policy**.
   b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
   c. In the **Policy Overview** screen, enter a policy name and policy description.
   d. Select **Application**.
   e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b. For the device on which you have to enable SD-AVC, click **…** and select **Edit** from the menu.

c. Click **Additional Templates**.

d. Add the localized policy created in an earlier step of this procedure.

e. Click **Update** and proceed through the next screens to push the updated template to the device.

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

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

or

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

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

Table 4: 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.

Before You Begin

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

Table 5: 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	Cisco-hosted	**Required credentials**: • Cloud gateway URL: Use: https://datamanagement-us01.sdwan.cisco.com/validate_sdavc/ • OTP: Use the Cisco Catalyst SD-WAN Portal to get the OTP. See the Cisco Catalyst SD-WAN Portal Configuration Guide for details. **Other requirements**: Enable SD-AVC in cluster management, as described here. **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	

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 https://datamanagement-us-01.sdwan.cisco.com/validate_sdavc/ 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 https://datamanagement-us-01.sdwan.cisco.com/validate_sdavc/ for the URL, and open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. **Other requirements**: Before enabling the Cloud Connector, enable SD-AVC in cluster management, as described here.

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

Enable Cisco SD-AVC Cloud Connector

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

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

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

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

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

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

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

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

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

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

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

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

   - Client ID

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

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

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

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

Create Credentials on the Cisco API Console

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

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

Note These credentials expire after 90 days.

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.

Software Installation and Upgrade for Cisco IOS XE Routers

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

Supported Hardware Platforms and Interface Modules

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

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

Supported Crypto Modules

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

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

Before You Begin

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

- The controller devices—Cisco SD-WAN Validators, Cisco SD-WAN Manager instances, and Cisco SD-WAN Controllers—are running Cisco Catalyst SD-WAN Software Release 18.3.
- If you deploy both IOS XE and vEdge routers in the overlay network, the vEdge routers are running Release 17.2.1 or higher of the Cisco Catalyst SD-WAN software. With these software versions, the vEdge and IOS XE software can interoperate, allowing BFD tunnels to be established between vEdge routers and IOS XE routers.
- If you deploy both IOS XE and vEdge routers in the same site, the vEdge routers are running Cisco Catalyst SD-WAN Software Release 18.3.
- The ISR 4000 series router has at least 4 gigabytes (GB) of DRAM installed. It is recommended that the router have 8 GB of DRAM.
- The ASR 1000 Cisco SD-WAN Validator series router has at least 8 GB of DRAM installed. The ASR 1002-HX router has at least 16 GB of DRAM installed.
- The router bootflash has a minimum of 1.5 GB space available for the XE SD-WAN image or, beginning with Cisco IOX SD-WAN Release 17.10, the router bootflash has a minimum of one half of its disk space available for the XE SD-WAN image.
- If using your enterprise root certificate to authenticate the router, the certificate is copied to the router's bootflash before installing the XE SD-WAN software.
- All unsupported modules are removed from the router before installing the XE SD-WAN software. For a list of supported modules, see Supported Interface Modules and Supported Crypto Modules.
- For information about deploying a Cisco ASR 1006-X with an RP3 module, see Cisco ASR 1006-X with an RP3 Module.
- The updated device list is uploaded to Cisco SD-WAN Manager and sent to the Cisco SD-WAN Validator. To do so:

  1. Obtain the router's chassis and board ID serial number by issuing the **show crypto pki certificates CISCO_IDEVID_SUDI** command at the system prompt. If running Release 16.6.1 or earlier on an ASR series router, issue the **show sdwan certificate serial** command.

2. Add the router's serial number to Plug and Play (PnP) Connect portal. See Add the IOS XE Router to the PnP Portal section for more details..
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**. Click **Sync Smart Account** to download the updated device list to Cisco SD-WAN Manager and send it to the Cisco SD-WAN Validator.

- Device configuration templates are created and attached to the router using Cisco SD-WAN Manager **Configuration** > **Templates**. This ensures that the router can obtain a configuration and establish full control connections when it comes up.
- If the router exceeds the unidirectional encrypted bandwidth of 250 Mbps and if the HSECK9 license is not already installed, the license file is copied to the router's bootflash and license installed on the router license install file path.
- The ASR 1000 series, ISR 1000 series, and ISR 4000 series router is running the required version of the ROM monitor software (ROMMON), as shown in the following table. To verify the ROMMON version running on the router, issue the **show rom-monitor** or **show platform** command at the system prompt.

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

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

Hardware Platform	CIMC	NFVIS
ISRv	3.2.4	3.8.1

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

Download the Cisco IOS XE Catalyst SD-WAN Software

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

1. Go to https://www.cisco.com.
2. Click **Support & Downloads** from the menu on the left side.
3. In the **Products and Downloads** page, in the **Downloads** search box, choose Software-Defined WAN (SD-WAN).
4. In the **Select a Product** page, from the right-most pane, choose **XE SD-WAN Routers**.

5. From the right-most pane, select your router model.
6. Click the desired software release version to download it. The software image name has the format *router-model*-ucmk9.*release-number*
7. Copy the software image to an HTTP or FTP file server in your local network.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Remove all existing configurations from the router.

```
Device# write erase
```

10. Set the config-register to 0x2102.

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

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

```
Device# show bootvar
```

12. Reboot the router.

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

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

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

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

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

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

    The default password can be used once and then must be changed. If the initial configuration session times out or if the session is interrupted or terminated before the password is changed and saved, subsequent login attempts fail. To restore login access to the device, you must reset the password to its default value through the local console in ROMMON mode. Then the initial provision process must be restarted. For information about restoring the password, see Recover the Default Password, on page 36.

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

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

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

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

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

```
Router# sh sdwan software
VERSION       ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
```

```
--------------------------------------------------------------------------------
16.12.1b.0.4  true    true     true      user       2019-09-21T00:24:22-00:00

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

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

```
Router# request platform software sdwan software reset

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

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

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

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

Configure IOS XE Router Using CLI

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

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

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

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

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

   ```
   Device# pnpa service discovery stop
   ```

3. Enter configuration mode:

   ```
   Device# config-transaction
   Device(config)#
   ```

4. Configure the system IP address.

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

   Cisco SD-WAN Manager uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

5. Configure the numeric identifier of the site where the device is located:

   ```
   Device(config-system)# site-id site-id
   ```

6. Configure the IP address of the Cisco SD-WAN Validator or a DNS name that points to the Cisco SD-WAN Validator. The Cisco SD-WAN Validator's IP address must be a public IP address, to allow the router to reach the Cisco SD-WAN Validator.

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

7. Configure the organization name, which is the name that is included in the certificates on all devices in the overlay network. This name must be the same on all devices.

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

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

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

Note

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

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

   ```
   Device(config)# interface GigabitEthernet  #
   Device(config)# ip address  ip-address mask
   ```

```
Device(config)# no shut
Device(config)# exit
```

10. Configure tunnel parameters:

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

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

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

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

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

13. Save the changes and exit configuration mode:

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

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

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

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

```
Device# show sdwan control connections

PEER    PEER PEER         SITE  DOMAIN  PEER         PEER PRIV  PEER        PEER PUB
TYPE    PORT SYSTEM IP    ID    ID      PRIVATE IP   PORT       PUBLIC IP   PORT
LOCAL COLOR
-------------------------------------------------------------------------------------------
vsmart  dtls 192.168.1.2  10    1       172.1.1.3    12346      172.1.1.3   12346
 biz-internet
vbond   dtls -             0    0       172.1.1.4    12346      172.1.1.4   12346
 biz-internet
vmanage dtls 192.168.1.3  10    0       172.1.1.2    12346      172.1.1.2   12346
 biz-internet

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

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

Add IOS XE Devices to the Plug and Play Portal

Table 6: Feature History

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

To add a device to the Plug and Play portal:

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

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

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

Upgrading or Downgrading ROMMON

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

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

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

To upgrade or downgrade ROMmon, follow these steps:

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

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

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

```
Device# dir bootflash
```

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

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

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

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

4. Upgrade (or downgrade) the ROMmon file on your device by using the upgrade command as shown in the following examples:

   - Example upgrade command if you loaded the ROMmon file into the device bootflash:

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

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

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

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

```
Device# Reload
```

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

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

Perform Factory Reset

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

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

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

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

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
```

```
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON

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

Recover the Default Password

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

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

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

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

   ```
   Device# confreg 0x2102
   ```
8. In the local console of the device, enter privileged exec mode.
9. Take either of these actions:
   - For Cisco IOS XE SD-WAN 16.10 releases beginning with release 16.10.4 or for Cisco IOS XE SD-WAN 16.12 releases beginning with release 16.12.2:

     ```
     Device# request platform software sdwan config reset
     Device# reload
     ```
   - For Cisco IOS XE SD-WAN 16.10 releases earlier than release 16.10.4 or for Cisco IOS XE SD-WAN 16.12 releases earlier than 16.12.2:

     ```
     Device# request platform software sdwan software reset
     ```
10. After the device comes back up, configure a new admin password.

Software Installation and Upgrade for vEdge Routers

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

Software Image Signing

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

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

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

Software image signing is available in Releases 16.1 and later.

Software Version Compatibility

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

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

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

Install the Software

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

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

- To install software on a Cisco SD-WAN Validator, see *Create Cisco SD-WAN Validator VM Instance on ESXi* or *Create Cisco Catalyst SD-WAN Validator VM Instance on KVM*. During the process of creating the VM, you install the vBond.ova file.

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

Upgrade the Software

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

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

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

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

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

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

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

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

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

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

Best Practices for Software Upgrades

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

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

- If the new software images are located on an FTP server, ensure that the FTP server can handle concurrent file transfers.
- If the new software images are in the image repository on Cisco SD-WAN Manager, ensure that the WAN in which Cisco SD-WAN Manager is located has sufficient capacity for concurrent file transfers.
- You cannot include Cisco SD-WAN Manager in a group software upgrade operation. You must upgrade and reboot Cisco SD-WAN Manager server by itself.
- In a group software upgrade operation, you can upgrade up to 40 Cisco vEdge devices or Cisco IOS XE Catalyst SD-WAN devices and reboot or activate upto 100 Cisco vEdge devices or Cisco IOS XE Catalyst

SD-WAN devices simultaneously (when the new image is available locally). These maximum numbers assume that Cisco SD-WAN Manager is idle and only upgrade and reboot operations are being carried out. In case of other management tasks occuring on Cisco SD-WAN Manager at the same time, the number of available sessions reduces.

- When you are setting a software image to be the default software image, activate it first, before making it the default image.

Obtain Software Images from Cisco Catalyst SD-WAN

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

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

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

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

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

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

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

Add New Software Images to the Repository

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

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2.
3. Click **Add New Software**, and select the location from which to download the software image. The location can be:
   - Cisco SD-WAN Manager—To select an image stored on the local Cisco SD-WAN Manager.
   - Remote Server (preferred) —To select an image stored on a remote file server.
   - Remote Server – Cisco SD-WAN Manager—To select an image stored on a remote Cisco SD-WAN Manager. This location is available in Releases 17.2 and later.
4. If you select Cisco SD-WAN Manager, the Upload Software to Cisco SD-WAN Manager dialog box opens.
   a. Click **Browse** to select the software images or **Drag and Drop** the images for vEdge routers, Cisco SD-WAN Controllers, or Cisco SD-WAN Manager.
   b. Click **Upload** to add the images to Cisco SD-WAN Manager repository.
5. If you select Remote Server, the Location of Software on Remote Server dialog box opens.
   a. Enter the version number of the software image.
   b. Enter the URL of the FTP or HTTP server on which the images reside.
   c. Click **OK** to point to the software images on the remote host.
6. If you select Remote Server – Cisco SD-WAN Manager, the Upload Software to Cisco SD-WAN Manager dialog box opens.
   a. Enter the hostname of the Cisco SD-WAN Manager server.
   b. Click **Browse** to select the software images or **Drag and Drop** the software image for vEdge routers, Cisco SD-WAN Controllers, or Cisco SD-WAN Manager.
   c. Click **Upload** to add the images to Cisco SD-WAN Manager repository.

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

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

Upgrade the Software Image

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

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

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

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

Activate a New Software Image

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

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

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

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

View Log of Software Upgrade Activities

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

1.
2.

Upgrade a Software Image from the CLI

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

To upgrade the software image from within the CLI:

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

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

2. Install the software:

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

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

   Specify the image location in one of the following ways:

   - The image file is on the local server:

     /*directory-path*/

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

   - The image file is on an FTP server.

     ftp://*hostname*/

   - The image file is on an HTTP server.

     http://*hostname*/

   - The image file is on a TFTP server.

     tftp://*hostname*/

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

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

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

   ```
   Viptela# request software activate
   ```

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

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

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

Redundant Software Images

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

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

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

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

```
Viptela# request software activate
```

Downgrade a Cisco vEdge Device to an Older Software Image

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

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

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

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

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

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

   - The image file is on the local server:

     /*directory-path*/

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

   - The image file is on an FTP server.

     ftp://*hostname*/

   - The image file is on an HTTP server.

     http://*hostname*/

   - The image file is on a TFTP server.

     tftp://*hostname*/

4. Set the installed image as the default.

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

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

```
vEdge# request software reset
```

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

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

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

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

```
vManage#show system status

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


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

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

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

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

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

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

```
Chassis serial number:   None
```

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

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

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

```
vManage1# show system status

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


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

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

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

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

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

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

Expand the Disk Size

Perform the following steps to increase the disk size on Cisco SD-WAN Manager.

1. Power the device down on all Cisco SD-WAN Manager instances in the cluster.

   ```
   request nms all stop
   ```

2. Power down the Cisco SD-WAN Manager VM.
3. Using the appropriate tools for the hypervisor system hosting the Cisco SD-WAN Manager VM, increase the size of the secondary partition that is used as the data disk partition.
4. Start the Cisco SD-WAN Manager VM.
5. Power the device down.

   ```
   request nms all stop
   ```

6. Use the following command to reconfigure Cisco SD-WAN Manager to use the new disk size.

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

   The partition resizing will take some time to complete.

7. Use the following vshell command to confirm that the /opt/data disk has been resized.

   ```
   vshell

   df -hk | grep data
   ```

8. Reboot the device.

For more details about the cluster upgrade processes, see Cisco Catalyst SD-WAN Manager Cluster Creation and Troubleshooting guide.

Use Software Maintenance Upgrade Package on Cisco IOS XE Catalyst SD-WAN Devices

Table 7: Feature History

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

Supported Devices for Software Maintenance Upgrade Package

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and later	• Cisco ISR 1000 Series Integrated Services Routers • Cisco IR1101 Integrated Services Router Rugged • Cisco ISR 4000 series Integrated Services Routers • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Series Edge Platforms • Cisco Catalyst 8000v Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and later	Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers

Information About Software Maintenance Upgrade Package

A Software Maintenance Upgrade (SMU) is a point fix for a critical bug in released software that attempts to minimize disruption to the router, if possible. An SMU is not designed to replace a maintenance release. The fix is delivered as an SMU package file. A package is provided for each release and each component of Cisco Catalyst SD-WAN. The package contains metadata that describes the content of the package and the fix for a reported issue that you request the SMU package for.

Each SMU image filename (SMU image) that is stored in the software repository includes the base image version and the defect ID of the fix. In the image name:

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

To install an SMU image on a Cisco IOS XE Catalyst SD-WAN device, follow these steps:

1. Download an SMU image for your release from the Cisco site, https://software.cisco.com.
2. Perform one of the following actions to upload an SMU image:
   - Upload an SMU image by adding the image to the device software repository using Cisco SD-WAN Manager. For more information about adding, viewing, and activate an SMU image, see Manage Software Maintenance Upgrade Images, on page 50.
   - Upload an SMU image by copying the image to the bootflash of your device using the CLI. For more information about installing and activating an SMU image using the CLI, see Manage Software Maintenance Upgrade Images Using the CLI, on page 51.
3. Upgrade or install and activate an SMU image on a device.
   - Install: The desired SMU image is installed on the device.
   - Activate: The installed SMU image is activated, which results in rebooting the device.

Note The device reboot occurs based on whether the SMU image type is hot or cold. For more information about the SMU package types, see SMU Types, on page 49.

If the SMU image is compatible with the Cisco IOS XE Software image on the device, the upgrade task is successful and the SMU image is installed and activated on the device. If the upgrade task is not successful, the device automatically reverts to the state that it was in before the SMU image activation.

The following are the steps to deactivate and remove an SMU image from a Cisco IOS XE Catalyst SD-WAN device:

1. Deactivate a currently active SMU image on a Cisco IOS XE Catalyst SD-WAN device and wait for the status to change from "Active" to "Installed" in Cisco SD-WAN Manager.

   If the SMU image deactivation on a device fails, the device automatically reverts to the state that it was in before the image deactivation.

2. Remove an SMU image from a device and have the base image version (Cisco IOS XE image version) on the device.

   Ensure that you deactivate the SMU image before you remove it.

Cisco SD-WAN Manager receives several notifications during the SMU image upgrade and you receive success or failure messages, as applicable. Use the Task View window to see these messages.

SMU Types

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

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

Benefits of Using Software Maintenance Upgrade Package

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

Manage Software Maintenance Upgrade Images

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

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

Add, View, and Activate an SMU Image

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

   See the Cisco SD-WAN Manager Add Software Images to Repository procedure in the *Cisco Catalyst SD-WAN Monitoring and Operations* guide.

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

   See theCisco SD-WAN Manager View Software Images procedure in the *Cisco Catalyst SD-WAN Monitoring and Operations* guide. Note the following points when viewing SMU images:

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

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

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

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

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

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

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

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

Deactivate or Remove an SMU Image

Deactivate an SMU image and remove the image from a device by using the Cisco SD-WAN Manager software upgrade window. See the Deactivate an SMU Image procedure in the Cisco Catalyst SD-WAN Monitoring and Operations guide.

Manage Software Maintenance Upgrade Images Using the CLI

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

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

Install and Activate an SMU Image Using the CLI

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

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

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

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

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

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

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

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

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

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

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

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

Deactivate and Remove an SMU Image Using the CLI

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

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

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

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

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

3. Confirm that the SMU image can be deactivated.

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

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

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

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

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

- Check the upgrade and confirm the configuration:

  ```
  show sdwan running system
  ```

- Add and upgrade the confirm timer:

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

- Execution commands:

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

Verify Status of Software Maintenance Upgrade Images

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

Monitor SMU Status Using Cisco SD-WAN Manager

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

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

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

Verify SMU Status Using the CLI

Example 1:

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

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


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

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

Example 2:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Example 3:

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

```
Device# show install package bootflash:
c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
```

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