Managing the SD-Routing Device Using Cisco SD-WAN Manager

This chapter includes information about managing and monitoring the SD-Routing devices using Cisco SD-WAN Manager. It contains the following sections:

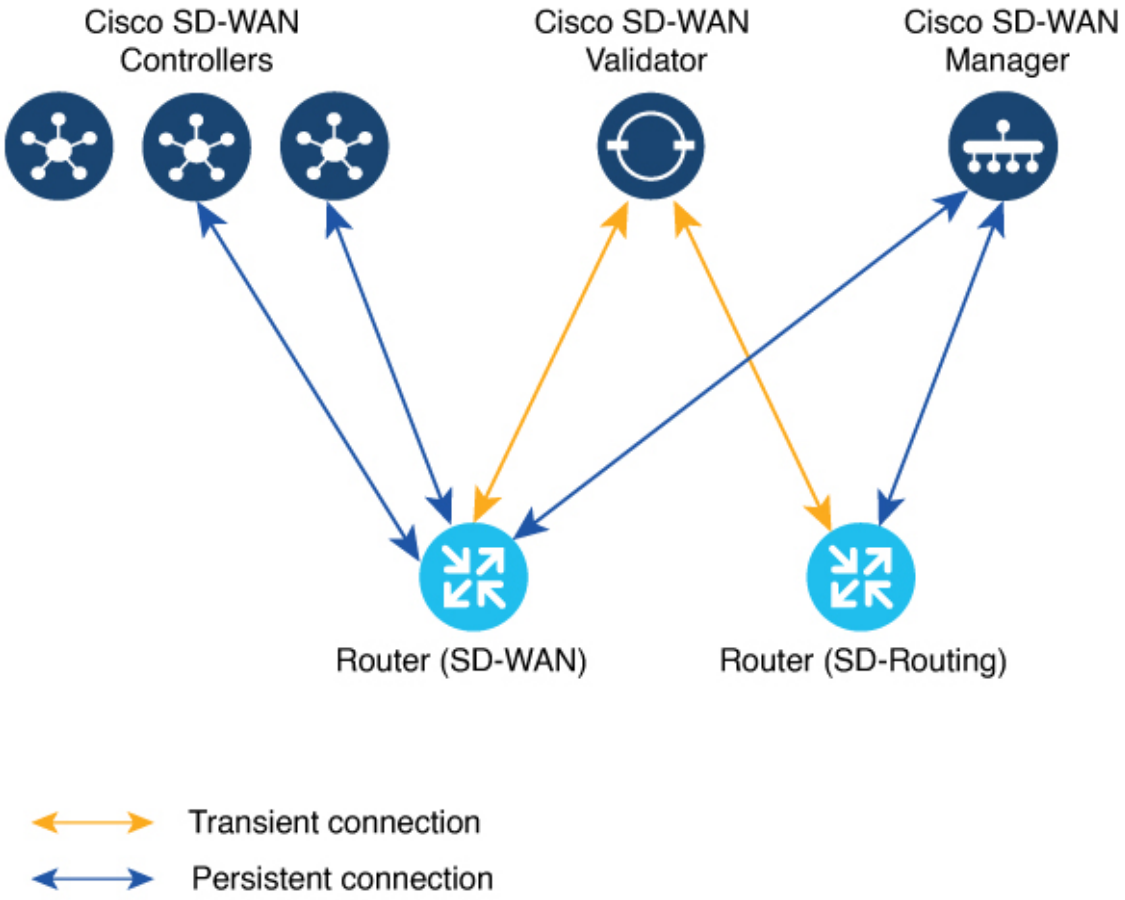
Information About Using Cisco SD-WAN Manager to Monitor the SD-Routing Devices

This feature allows you to perform the basic management capabilities through Cisco SD-WAN Manager on the Cisco IOS XE devices that are operating in non-SD-WAN mode. From Cisco IOS XE 17.12.1a onwards, such devices will be referred as SD-Routing devices. You can use a single Network Management System (NSM) (Cisco SD-WAN Manager) to manage and monitor all the Cisco IOS XE routers and help in simplifying solution deployments.

Note Cisco IOS-XE Software No Payload Encryption (NPE) or No Lawful Intercept and No Payload Encryption (NOLI/NPE) images does not support managing the SD-Routing devices using Cisco SD-WAN Manager feature.

Note The minimum software version required for this feature to work is Cisco IOS XE 17.12.1a and Cisco SD-WAN Release 20.12.1.

Figure 1: Managing the SD-Routing Devices



Benefits of Managing the SD-Routing Devices Using Cisco SD-WAN Manager

1. Use of a single NMS (Cisco SD-WAN Manager) for Cisco Catalyst SD-WAN and SD-Routing deployments in an Enterprise network.
2. Co-existence of Cisco SD-WAN and SD-Routing devices on the same Cisco SD-WAN Manager.

Prerequisites

The following are the prerequisites to onboard the SD-Routing devices:

- Ensure that the device run the Cisco IOS XE 17.12.1a image in install mode. For more information on the modes, see the Modes Using Cisco CLI section.
- A Cisco SD-WAN Manager instance either on-prem or hosted on a cloud.
- Connectivity from the device to the Cisco SD-WAN Manager.
- Enable netconf-yang models for enabling DMI which is required for managing from Cisco SD-WAN Manager.
- Devices operating in autonomous mode must be configured with the following basic configuration manually to establish the secure control connections with controllers (Cisco SD-WAN Validator and Cisco SD-WAN Manager):
  - System properties:
    - System-ip
    - Site-id
    - Organization-name
    - Cisco SD-WAN Validator information (IP address or FQDN Cisco SD-WAN Validator server)
  - Interface configuration:
    - Physical interface with a static or dynamic IP address and subnet mask
    - Dynamic routing or default route to provide reachability to Cisco SD-WAN Validator or Cisco SD-WAN Manager

Limitations

- Cisco SD-routing devices onboarding onto Cisco SD-WAN Manager is only supported with universalk9 images. No Payload Encryption (NPE) images are not supported.
- In Cisco IOS XE 17.12.1a release, basic monitoring is supported and additional features will be supported in the subsequent releases. For more information on supported features list, see the platform specific Release Notes.
- Cisco SD-Routing devices can only have one control connection to Cisco SD-WAN Manager from an interface with reachability to the controllers.
- Cicso SD-routing devices will not have any active connection with Cisco SD-WAN Controller.
- Dedicated management interface is not supported for the connection to the Cisco SD-WAN Manager.

Supported WAN Edge Devices

The table lists the supported WAN Edge platforms and onboarding options.

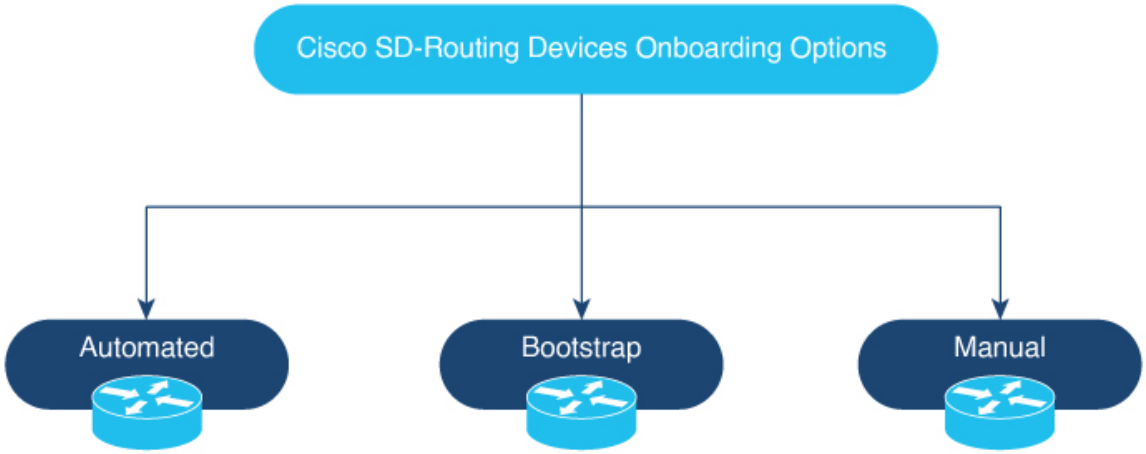
Table 1: Supported WAN Edge Platforms and Onboarding Options

Platforms	Automated	Bootstrap	Manual
Cisco ASR 1000 Series Aggregation Services Routers			
ASR1001-HX	Yes	Yes	Yes
ASR1002-HX	Yes	Yes	Yes
Cisco 4400 Series Integrated Services Routers			
Cisco 4431 ISR	Yes	Yes	Yes
Cisco 4451 ISR	Yes	Yes	Yes
Cisco 4461 ISR	Yes	Yes	Yes
Cisco 4300 Series Integrated Services Routers			
Cisco 4321 ISR	Yes	Yes	Yes
Cisco 4331 ISR	Yes	Yes	Yes
Cisco 4351 ISR	Yes	Yes	Yes
Cisco 4200 Series Integrated Services Routers			
Cisco 4221 ISR	Yes	Yes	Yes
Cisco 100 Series Integrated Services Routers			
Cisco 1000 ISR	Yes	Yes	Yes
Cisco Catalyst 8000V Series Edge Platforms			
Cisco Catalyst 8000V	Not applicable **Note** Automated onboarding is applicable only for the hardware device.	Yes	Yes
Cisco Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	Yes	Yes	Yes
C8200L-1N-4T	Yes	Yes	Yes
Cisco Catalyst 8300 Series Edge Platforms			
C8300-1N1S-4T2X|6T	Yes	Yes	Yes
C8300-2N2S-4T2X|6T	Yes	Yes	Yes

Platforms	Automated	Bootstrap	Manual
Cisco Catalyst 8500 Series Edge Platforms			
C8500-12X4QC	Yes	Yes	Yes
C8500-12X	Yes	Yes	Yes
C8500L-8S4X	Yes	Yes	Yes
C8500-20X6C	Yes	Yes	Yes

Onboarding the SD-Routing Devices

This section explains the workflows to onboard the SD-Routing devices:



- Onboarding the SD-Routing Devices
  - Automated Onboarding: Uses the Dynamic Host Configuration Protocol (DHCP) and Cisco Plug and Play (PNP) to automatically onboard the device to Cisco SD-WAN Manager.
  - Bootstrap Onboarding: Uses the bootstrap file either on the bootflash or on a USB and configures the device with the minimum configuration to reach the Cisco SD-WAN Manager.
  - Manual Onboarding: Configures the device manually using IOS-XE commands to onboard the device to Cisco SD-WAN Manager.

To onboard the SD-Routing devices, the prerequisites are:

- System IP

For manual Onboarding, the prerequisites are:

- Site ID
- Organization-name

- Cisco SD-WAN Validator information (IP address or FODN Cisco SD-WAN Validator server)
- Interface for connection to Cisco SD-WAN Manager (Physical, Sub-interface, and Loopback)

Onboarding the SD-Routing Devices Using Automated Workflow

To onboard the SD-routing devices using the automated workflow, perform these steps:

- Configure the Plug and Play Connect Portal
- Configure the Cisco SD-WAN Manager using quick connect workflow
- Bring up the device in Day0 mode

Configuring the Plug and Play Connect Portal

To configure the PnP Connect portal, perform these steps:

Before you begin

Ensure that you can access to the PnP Connect portal and an active Smart Account and Virtual Account using your Cisco User ID. You have to also use a CCO ID that is associated as the Smart Account or Virtual Account admin of the account, on PnP Connect portal.

Note You can enable the PnP Connect Sync only after you enter the Smart Account credentials in the Cisco SD-WAN Manager Settings page.

Step 1 Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.

Step 2 Create a Controller Profile and upload the **root-ca** if it is for an Enterprise network.

Note If the overlay network is **Cisco PKI**, you do not have to upload any certificate.

Step 3 Enter the Controller Profile with controller type as VBond and click **Next**.

Step 4 Enter the required parameters in the **Add Controller Profile** and click **Next**.

Step 5 Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.

Configuring the Cisco SD-WAN Manager Using Quick Connect Workflow

To configure the Cisco SD-WAN Manager using Quick Connect workflow, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, go to **Workflows** > **Quick Connect**.

Step 2 Click **Get Started**.

Step 3 Click **Next**.

Step 4 If you have not uploaded the provisioning file (*.csv* or *.viptela*) from PnP to Cisco SD-WAN Manager, you can use either **.csv upload** or **.viptela upload** or **Sync Smart Account** option to add the device to Cisco SD-WAN Manager. If the device is already added to Cisco SD-WAN Manager, select the **skip for now** option.

Note The *.csv* file is applicable only for hardware devices. The *.viptela* file is applicable for both hardware and software devices.

Step 5 Click **Sync Smart Account** if you have not syncrnized it already. You should now see your device listed in the table of the devices.

Click Sync Smart Account,

Step 6 Click **Next**.

Step 7 In the Add and Review Device Configuration dialog box, enter the Site-ID, System-IP, Hostname, and click **Apply**.

Step 8 Click **Next**.

Step 9 Add any option Tag and click **Next**.

Step 10 To verify the device that is added , choose **Configuration**> **Devices** and click enable **Device Model** in Table Settings.

Step 11 A list of routers in the network is displayed, showing detailed information about each router. To verify that the devices are added, select **Configuration** > **Certificates**.

Bringing Up the SD-Routing Device

To bring up the SD-Routing device, perform these steps:

Step 1 Bring up the device in Day-0 state. If the device is not in Day-0 state, use either **controller-mode reset** or **writer erase** with **reload** option to bring it to Day-0 state.

Step 2 Ensure that the device gets the IP address over DHCP on one of the interfaces other than the Gigabit Etherner0 interface. Also, ensure that the device is reachable to devicehelper.cisco.com and the Cisco SD-WAN Validator.

Note Dedicated management interface is not supported for the connection to the Cisco SD-WAN Manager.

Step 3 The device control connection comes up on Cisco SD-WAN Manager.

Step 4 Verify the control connection status on the Edge device using the**show sd-routing connections summary** command:

Example:

```
Router#show sd-routing connections summary

PEER                                          PEER
PEER     PEER  PEER             SITE        PEER                                  PRIV
PEER                                    PUB
TYPE     PROT  SYSTEM IP        ID          PRIVATE IP                            PORT   PUBLIC
IP                               PORT   STATE   UPTIME
------------------------------------------------------------------------------------------------
Cisco SD-WAN Manager  dtls  172.16.255.22    200         10.0.12.22
12446  10.0.12.22                            12446  up      12:05:29:3
```

Step 5 Verify the control connection status on Cisco SD-WAN Manager.

Onboarding the SD-Routing Devices Using Bootstrap

To onboard the SD-Routing device using the bootstrap, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, go to **Workflows** > **Quick Connect**.

Step 2 Click **Get Started**.

Step 3 Click **Next**.

Step 4 If you have not uploaded the provisioning file (*.csv* or *.viptela*) from PnP to Cisco SD-WAN Manager, you can use either **.csv upload** or **.viptela upload**or **Sync Smart Account** option to add the device to Cisco SD-WAN Manager. If the device is already added to Cisco SD-WAN Manager, select the **skip for now** option.

Note The *.csv* file is applicable only for hardware devices. The *.viptela* file is applicable for both hardware and software devices.

Step 5 Select the device that you want to onboard and click **Next**.

Step 6 In the Add and Review Configuration dialog box, enter the Site-ID, System-IP, Hostname, and click **Apply**.

Step 7 To verify the device that is added, choose **Configuration**> **Devices** and click enable **Device Model** in Table Settings.

Step 8 Ensure that the device is in valid state from **Configuration** > **Certificate** page.

Step 9 From the Cisco SD-WAN Manager menu, choose **Configuration**> **Devices**.

Step 10 For the Cisco SD-Routing software devices (Cisco c8000V), perform these steps to generated the bootstrap and onboard the device:

Note For hardware devices, follow the instructions in Step 11.

a) Click **...** at the right pane of the window and choose **Generate Bootstrap Configuration**.

b) Choose Cloud-init option and enter a name for the WAN Interface Name and click **OK**.

Note Ensure that the DHCP is enabled on the selected interface and is reachable to Cisco SD-WAN Validator and Cisco SD-WAN Manager. Also, for the software device, use only Gigabit Ethernet1interface as the VPN0 interface.

c) Click **Download** to download the image on the device.

Example:

Sample image: ciscosdwan_cloud_init.cfg

Sample image with Certificate : ciscosdwan_cloud_init_with_ent_cert.cfg

d) For cloud-based controllers, the downloaded bootstrap file can be added as a user data field when you deploy the device. It will bring up the controller in SD-Routing mode and establish the connection with Cisco SD-WAN Validator and Cisco SD-WAN Manager.

Step 11 For hardware devices, perform these steps to generate the bootstrap and onboard the device:

a) From the Cisco SD-WAN Manager menu on the device page, click **Export Bootstrap Configuration**.

b) Select the check box for SD-Routing. In the **Export Bootstrap Configuration** dialog box, enter the **WAN Interface name**.

Note The management interface name may vary among Cisco IOS XE device models. Specify the interface name based on the model you wish to onboard and which can reach the Cisco SD-WAN Validator and Cisco SD-WAN Controller.

c) Click **Generate Generic Configuration** to download the generic *.cfg* bootstrap applicable for the hardware devices. Unzip the file and rename it as *ciscosdawn.cfg*.

Note Ensure that the DHCP is enabled on the selected interfaces and is reachable to Cisco SD-WAN Validator and Cisco SD-WAN Manager.

The bootstrap file will contain the organization name, Cisco SD-WAN validator IP, and root-ca certificates. For the enterprise network, it will have the enterprise root-ca- certificates.

d) Copy the bootstrap file to the device bootflash as *ciscosdwan.cfg*.

e) Execute the **sd-routing bootstrap load bootflash:ciscosdwan.cfg** command.

Example:

```
Router# sd-routing bootstrap load bootflash:ciscosdwan.cfg
Located the file. Beginning to extract the data
Extraction summary
-Organization name - "aniltb2"
-Interface - GigabitEthernet0/0/0
-vbond  - 99.99.1.51
Successfully extracted root-cert info

Do you want to proceed and apply extracted
parameters to enable sd-routing feature?? (yes/[no]): yes
Successfully configured bootstrap extracted parameters
Router#
*May 10 08:56:11.159: %SYS-5-CONFIG_P: Configured programmatically by process Exec from console as console
*May 10 09:05:11.751: %DMI-5-AUTH_PASSED: R0/0: dmiauthd: User 'vmanage-admin' authenticated successfully from
201.201.201.1:41902  for netconf over ssh. External groups
```

f) Verify the control connection using these **show sd-routing system status**, **show sd-routing system status**, and **show sd-routing local-properties summary** commands.

Onboarding the Devices Manually

To onboard the SD-Routing devices manually, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, go to **Workflows** > **Quick Connect**.

Step 2 Click **Get Started**.

Step 3 Click **Next**.

Step 4 If you have not uploaded the provisioning file (*.csv* or *.viptela*) from PnP to Cisco SD-WAN Manager, you can use either **.csv upload** or **.viptela upload** or **Sync Smart Account** option to add the device to Cisco SD-WAN Manager. If the device is already added to Cisco SD-WAN Manager, select the **skip for now** option.

Note The *.csv* file is applicable only for hardware devices. The *.viptela* file is applicable for both hardware and software devices.

Step 5 Select the device that you want to onboard and click **Next**.

Step 6 In the Add and Review Configuration dialog box, enter the Site-ID, System-IP, Hostname, and click **Apply**.

Step 7 To verify device that is added , choose **Configuration**> **Devices** and click enable **Device Model** in Table Settings.

Step 8 A list of routers in the network is displayed with detailed information about each router. To verify that the devices are added, select **Configuration** > **Certificates**.

Step 9 Preform one of the following steps based on the device that you want to onboard manually:

a) For the hardware device, enter the initial day-0 configurations using the IOS command after a system boot up.

b) For the Cisco SD-Routing software devices, deploy the Cisco c8000v in Amazon Web Services (AWS) or Azure without the bootstrap.

Step 10 Configure the minimum parameters to enable the control connection on Cisco SD-WAN Manager.

Example:

```
netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org. Name%"
  site-id %id%
  system-ip %system ip%
  vbond name %vbond name or vbond ip%
  vbond port 12346
  wan-interface %uplink interface%

ip route 0.0.0.0 0.0.0.0 %next hop ip%

interface %uplink interface%
   ip address  %dhcp or static%
   no shutdown
```

Step 11 Configure the required parameter to enable the SD-Routing mode:

a) Ensure that the interface is configured with a static IP address or through DHCP. Also, the interface must be in **no shut** state.

b) Configure either Validator IP or Validator Name.

c) Configure the System-IP, Site-ID, Organization-Name and WAN-Interface.

Step 12 Verify that the feature is enabled by checking the status of the vdaemon.

Example:

```
Router# show platform software yang-management process state
Confd Status: Started


Process               Status              State
------------------------------------------------------
nesd                  Running             Active
syncfd                Running             Active
ncsshd                Running             Not Applicable
dmiauthd              Running             Active
nginx                 Running             Not Applicable
ndbmand               Running             Active
pubd                  Running             Active
```

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
  Kernel time      : 347183
  Priority         : 20
```

```
Virtual bytes    : 405110784
Resident pages   : 12195
Resident limit   : 18446744073709551615
Minor page faults: 716496
Major page faults: 9130
```

Step 13 If the overlay network is for an enterprise, install the root certificates using the **request platform software sd-routing root-cert-chain install bootflash:cacert.pem** command. If the Cisco SD-WAN Manager is configured with Enterprise Certificates instead of **Cisco PKI**, you must install the root certificate on the device.

Step 14 Perform one of the following steps based on the device:

a) For Cisco 8000v device, copy the root certificate from the CA to Cisco 8000v.

b) Cisco devices are loaded with PKI and symantec root-certificates by default. If you need to install the enterprise root-certificate, install the certificate using the **request platform software sd-routing root-cert-chain install** <*path-to-root-cert*> command.

Example:

```
Device# request platform software sd-routing root-cert-chain install bootflash:ctrl_mng/cacert.pem
```

Step 15 Install the client enterprise certificates.

Note By default, the certificates will be loaded on the hardware devices. This step is only applicable for manually onboarding the software devices.

Step 16 Generate a Certificate Signed Request (CSR) for the device using the **request platform software sd-routing csr upload** <*bootflash:ctrl_mng/test*> command. You can specify any name for the folder that is created within the *bootflash:ctrl_mng/* directory.

Step 17 Copy the generated CSR file to the directory where you have the Enterprise CA. You can sing the certificate using the root key and root CA certificate and generate the pem certificate file.

Step 18 Copy the generated *certificate.pem* file to the device and use the **request platform software sd-routing certificate install** <*path-to-certificate-file*> command to install the certificate in the device.

Step 19 Verify the installation status of the certificates.

Example:

```
SJC_Primary# show sd-routing local-properties summary
….....
certificate-status               Installed
certificate-validity             Valid
certificate-not-valid-before     Apr 25 00:55:28 2023 GMT
certificate-not-valid-after      Apr 24 00:55:28 2024 GMT
….........
dns-name                         Validator
site-id                          100
tls-port                         0
system-ip                        172.16.255.11
chassis-num/unique-id            C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                       12345707
```

Step 20 Onboard the device on Cisco SD-WAN Manager. When you install the client certificate, ensure that you add the following in Cisco SD-WAN Manager .

a) Get the Chassis number and Serial number. To get the Chassis number and Serial number, use the s**how sd-routing local-properties** or **show sd-routing certificate serial** command.

```
Router# show sd-routing local-properties summary
chassis-num/unique-id            C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                       12345707
```

b) Upload the chassis-id using the **request vedge add chassis-num** <*Chassis id*> **org-name** <*Org Name*> **serial-num** <*Serial number from c8kv*> command on all the controllers.

Or

c) Create a *.viptela* file using the chassis number and serial number and upload the file to Cisco SD-WAN Manager and send to controllers.

Step 21 Verify the control connection status on Cisco SD-WAN Manager.

Example:

```
Router#show sd-routing connections summary

PEER                                          PEER
PEER     PEER  PEER             SITE        PEER                                  PRIV
PEER                                    PUB
TYPE     PROT  SYSTEM IP        ID          PRIVATE IP                            PORT   PUBLIC
 IP                                PORT   STATE   UPTIME
------------------------------------------------------------------------------------------------
vmanage  dtls  172.16.255.22    200         10.0.12.22                            12446
10.0.12.22                              12446  up      12:05:29:3
```

Onboarding the Device by Activating the Chassis Using the Token

To activate the chassis number, perform these steps:

Note This method is supported only on Cisco SD-WAN software devices (Cisco c8000v).

Step 1 Add the device to Cisco SD-WAN Manager using PnP Smart Sync method.

Step 2 Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.

Step 3 Create a controller profile and upload the **root-ca** if it is for an Enterprise network.

Step 4 Enter the controller type as vBond and click **Next**.

Step 5 Enter the required parameters in the **Add Controller Profile** and click **Next**.

Step 6 Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.

Step 7 From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.

Step 8 Go to **Smart Account Credentials** and click **Edit**.

Step 9 Enter the **Username** and **Password** and click **Save**.

Step 10 You can import the device list from PnP Connect Portal using these methods:

a) Go to **Configuration** > **Devices** and click **Sync Smart account**.

Or

a) Upload the *.viptela* that is downloaded from PnP Connect. Go to **Controller profiles** and click **Download the Provisioning file**.

b) From the Cisco SD-WAN Manager menu, choose **Configuration**> **Devices** > **Upload WAN Edge List**.

Step 11 The device will be in autonomous mode with startup config. The device will not be in Day0 mode.

Step 12 Apply the minimum configuration on the device.

Example:

```
netconf-yang
!
sd-routing
 no ipv6-strict-control
 organization-name "vIptela Inc Regression"
 site-id 500
 system-ip 172.16.255.15
 vbond ip 10.0.12.26
 vbond port 12346
 wan-interface GigabitEthernet2
!
ip route 0.0.0.0 0.0.0.0 10.0.5.13
!
ip interface GigabitEthernet2
 ip address 10.0.5.11 255.255.255.0
 no shutdown
!
```

Step 13 From the Cisco SD-WAN Manager menu, choose **Configuration**> **Certificates** and get the UUID and One Time Password (OTP) of the device you want to onboard.

Step 14 To override the chassis number that is generated by the software device, use the **request platform soft sd-routing activate chassis** <*newly uploaded chassis id*> **token** <*token generated by Cisco SD-WAN Manager*> command.

Step 15 If the overlay network is for an enterprise, install the enterprise-root certificates using the request platform **software sd-routing root-cert-chain install bootflash:cacert.pem** command. If the overlay network is **Cisco PKI**, you do not have to install the root certificate.

Note You do not have to generate a Certificate Signing Request (CSR) and sign it. The CSR will be generated while executing the step 14.

Step 16 Verify the control connection status on the Edge device using these commands:

Example:

```
show sd-routing local-properties summary
show sd-routing local-properties wan ipv4
show sd-routing connections summary
show sd-routing connections history
```

Onboarding the Multi-Tenancy SD-Routing Devices

This section explains the workflows to onboard the Multi-Tenancy SD-Routing devices:

- Automated Onboarding
- Manual Onboarding

Onboarding the Multi-Tenancy SD-Routing Devices Using Automated Workflow

To onboard the a multi-tenancy SD-Routing device, perform these steps:

Step 1 Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.

a) Create a virtual account.
b) Create a controller profile and upload the root-ca if it is for an Enterprise network.
c) Enter the controller type as vBond and click **Next**.
d) Enter the required parameters in the **Add Controller Profile** and click **Next**.
e) Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.

Or

Step 2 From the Cisco SD-WAN Manager menu, go to **Workflows** > **Quick Connect**.

Step 3 Click **Get Started**.

Step 4 Click **Next**.

Step 5 If you have not uploaded the *.csv* file to Cisco SD-WAN Manager, you can use one of the upload options to upload the file. Select **skip for now** option if you have uploaded the file.

Step 6 Click **Sync Smart account** or **.csv upload** or **.viptela upload**. You should now see your device listed in the table of devices.

Step 7 For Software device, generate bootstrap file as explained in previous section and add it as c8000v user config file.

Note For Multi-tenant setup, the System-IP must be configured only through quick connect workflow. You should not configure the system-IP using the CLI option.

Step 8 Based on the device type, perform one of these steps:

a) For the software device, deploy the Cisco c8000v in Azure or AWS and enter the bootstrap file either as custom data or user data input.
b) For hardware device, bring up the device in Day-0 state. If the device is not in Day-0 state, use either **controller-mode reset** or **writer erase** with **reload** option to bring it to Day-0 state.

Step 9 The device comes up with the Cisco SD-WAN Manager.

Step 10 To verify the status of the device, use the **show sd-routing connection summary status** and **show sd-routing local-properties summary** commands.

Onboarding the Multi-Tenancy SD-Routing Devices Manually

To onboard the Multi-Tenancy SD-Routing device manually, perform these steps:

Step 1 Deploy the Cisco Catalyst 8000v in Azure or AWS in autonomous mode.

a) Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.
b) Create a virtual account.
c) Create a controller profile and upload the root-ca if it is for an Enterprise network.
d) Enter the controller type as vBond and click **Next**.
e) Enter the required parameters in the **Add Controller Profile** and click **Next**.

f) Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.

Step 2 Configure the minimum parameters to enable Netconf-Yang:

Example:

```
config terminal
 netconf-yang
end
```

Step 3 Check the status of the Netconf-Yang using the **show platform software yang-management process state** command.

Step 4 Configure the required parameter to enable the Cisco SD-Routing mode:

a) Ensure that the interface is configured either with static IP address or through DHCP. Also, the interface must be in **no shut** state.

b) Configure either Cisco SD-WAN Validator IP or Cisco SD-WAN Validator name.

c) Configure the Cisco SD-WAN Validator, Site-ID, Organization-Name and WAN-Interface.

Note For Multi-tenant setup, the System-IP must be configured only through quick connect workflow. You must not configure the System-IP using the CLI option. However, you can use the CLI option to configure the SP Organization Name for SD-Routing devices in Multi-tenant deployment. The organization name refers to tenant's organization name for Multi-tenant deployment. It is visible only under the **show sd-routing local-properties summary** command after the device is onboarded.

Step 5 Verify that the feature is enabled by checking the status of the vdaemon.

Example:

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
  Kernel time      : 347183
  Priority         : 20
  Virtual bytes    : 405110784
  Resident pages   : 12195
  Resident limit   : 18446744073709551615
  Minor page faults: 716496
  Major page faults: 9130
```

Step 6 Verify the SD-Routing configurations in the Edge device. Also, get the chassis number for signing and upload to Cisco SD-WAN Manager WAN Edge List.

Step 7 To verify the status of the device, use this**show sd-routing local-properties summary** command.

Step 8 Copy the root-ca-chain.crt certificate from Cisco SD-WAN Manager into SD-Routing device.

Note This step is required only if you are using Enterprise certificate method. You can skip this step if you are using **Cisco PKI** method.

Step 9 Install the *root-ca-chain.crt* in SD-Routing device.

Step 10 Upload the provision file (*.Viptela*) from PnP to Cisco SD-WAN Manager WAN Edge List and send to controllers.

Step 11 Create a *.viptela* file using the chassis number, serial number and sign it. Upload the file to Cisco SD-WAN Manager and send to controllers.

Step 12 Get the Token from Cisco SD-WAN Manager. To onboard the device by establishing the control connection with Cisco SD-WAN Validator and Cisco SD-WAN Manager, use the **request platform software sd-routing activate chassis-number** <*chassis-num*> **token** <*token*> command.

Step 13 To verify the status of the device, use the **show sd-routing connection summary status** and **show sd-routing local-properties summary** commands.

Onboarding the Device to Cisco SD-WAN Manager Using One Touch Provisioning

To perform the one touch provisioning for a device, follow these steps:

Before you begin

When you configure a device by using the one touch provisioning, ensure that the process meets these requirements:

- Device must be in autonomous mode. You should stop the PnP discovery and device must have either a start up configuration or any configuration. The device should not be in Day-0 state.
- Device must be configured to reach Cisco SD-WAN Validator and Cisco SD-WAN over the WAN interface.

  Device must have the minimum required configuration for SD-Routing feature to communicate with controllers.

Also, onboarding the device to Cisco SD-WAN Manager using One Touch Provisioning method eliminates these steps to add the device:

- Adding WAN Edge device to Cisco SD-WAN Manager by using .**csv** or **.viptela** or **sync smart account**.
- Cisco device must be configured in SD-routing mode. You have to use the Manual or Bootstrap method to configure the device without adding the device to Cisco SD-WAN Manager.

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and enable One Touch Provisioning.

Step 2 Check if **One Touch Provisioning** is **Enabled**. If **Enabled**, go to Step 5.

Step 3 If **One Touch Provisioning** is **Disabled**, click **Edit**.

Step 4 For the **Enable Claim WAN Edges** setting, choose **Enabled** and click **Save**.

Step 5 Go to **Configuration** > **Devices** > **Unclaimed Devices**.

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

b) The device is removed from **Unclaimed Devices List** and listed on **WAN Edge List**.

Step 6 To verify the status of the device, use these **show sd-routing system status** , and **show sd-routing local-properties summary** commands.

Unprovisioning the Feature

To unprovision the feature, perform these steps:

Step 1 Remove the SD-Routing feature configuration from the device.

Example:

Note This option will delete all the certificates. You have to reinstall all the certificates.

Example:

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no sd-routing
Warning! Disabling this feature will result in deleting client certificates. Please backup the
certificates and use the CLIs to reinstall them on enabling this feature again.
Do you want to continue? (y/n)[n]: y
```

Step 2 Invalidate the device. For instructions, see the step 4 from the Onboarding the Devices Manually, on page 9 section.

Step 3 To delete the device:

a) From the Cisco SD-WAN Manager menu, choose **Configuration**> **Devices**.
b) Click **WAN Edge List** and choose the device that you want to delete.
c) Click **Delete WAN Edge**.
d) Read the message and click **Yes**.

Software Image Management

This section explains the process to upgrade the software image. Cisco SD-WAN Manager supports uploading a prepackaged Cisco virtual machine image, *tar.gz*, or an image in *qcow2* format. It is mandatory to upload a scaffold file if you choose a *qcow2* image file. Similarly, you can now select either an image package file or a *qcow2* image file with a scaffold file when configuring a Virtual Network Function (VNF) during service chain creation. Cisco SD-WAN Manager communicates with NETCONF that uses a simple Remote Procedure Call to retrieve operational data when an autonomous mode device is onboarded in Cisco SD-WAN Manager. (NETCONF) is a standard transport protocol that communicates with network devices. NETCONF provides mechanisms to edit configuration data. Cisco SD-WAN Manager upgrade workflow for the SD-Routing device is similar to the Controller mode Workflows.

Note The minimum software version required for this feature to work is Cisco IOS XE 17.12.1a.

Software Upgrade Using CLI

To upgrade the software, perform these steps:

Before you begin

- Disk Space Check: Checks for available bootflash space for downloading and expanding image.
- Image repository Check: Checks for remote server reachability.
- Auto Boot Enable: Checks if auto boot is enabled on the device.

Step 1 Download the Cisco IOS XE Release 17.12 image from the software page https://software.cisco.com.

Step 2 Upload the image to the device.

Step 3 Install the new software using the **install add file <bootflash:/file name> activate commit** command and activate.

Example:

```
Device# install add file <bootflash:/c8000v-universalk9.17.12.01.0.166070.SSA.bin activate commit
```

The device reloads when the activation is complete.

Note This is an interactive command and it prompts to review and accept it. This command fails if there is any unsaved configuration in the device. You will have to execute the **write memory** command and reinstall the software.

Step 4 Verify the upgrade using the **install commit** command.

Add Software Images to the Repository

Before you can upgrade the software on an SD-Routing device or Cisco SD-WAN Manager to a new software version, you need to add the software image to the Cisco SD-WAN Manager software repository. For more information on uploading the Cisco Catalyst 8000v Edge software to Cisco SD-WAN Controller using Cisco SD-WAN Manger and Remote server, see the Manage Software Repository section of the *Cisco SD-WAN Monitor and Maintain Configuration Guide.*

Software Upgrade Using Cisco SD-WAN Manager

To upgrade the software image on a device, perform these steps:

Before you begin

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see Downgrade a Cisco vEdge Device to an Older Software Image in the Cisco SD-WAN Getting Started Guide.
- If you want to perform a Cisco SD-WAN Manager cluster upgrade see, Upgrade Cisco vManage Cluster
- Auto Boot Enable: Checks if auto boot is enabled on device.

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.

Step 2 Click **WAN Edge**, **Control Components**, or **Manager** based on the type of device for which you wish to upgrade the software.

Step 3 In the table of devices, select the devices to upgrade by selecting the check box on the far left.

Note While upgrading Cisco SD-WAN Manager clusters, select all the nodes of the cluster in the table.

Step 4 Click **Upgrade**.

Step 5 In the **Software Upgrade** slide-in pane, do as follows:

a) Choose the server from which the device should download the image: **Manager**, **Remote Server**, or **Remote Server – Manager**.

Note
- If you chose **Remote Server**, ensure that the device can reach the remote server.
- When downloading an image from a remote server manually, ensure that only the following valid characters are used:
  - User ID: a-z, 0-9, ., _, -
  - Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
  - URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

b) For **SD-WAN Manager**, choose the image version from the **Version** drop-down list.

c) For **Remote Server – SD-WAN Manager**, choose the **vManage OOB VPN** from the drop-down list and choose the image version from the **Version** drop-down list.

d) Check the **Activate and Reboot** check box.

If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.

Note The **Activate and Reboot** option is not available while upgrading Cisco SD-WAN Manager software. You must activate the image after the upgrade task is completed and reboot Cisco SD-WAN Manager.

e) Click **Upgrade**

The device restarts, using the new software version, preserving the current device configuration. The **Task View** page opens, showing the progress of the upgrade on the devices.

Step 6 Wait for the upgrade process, which takes several minutes, to complete. When the **Status** column indicates Success, the upgrade is complete.

Step 7 From the Cisco SD-WAN Manger menu, choose **Maintenance** > **Software Upgrade** and view the devices.

Step 8 Click **WAN Edge**, **Control Components**, or **Manager** based on the type of device for which you wish to upgrade the software.

Step 9 In the table of devices, confirm that the **Current Version** column for the upgraded devices shows the new version. Confirm that the **Reachability** column says reachable.

Note

- If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image.
- If you upgrade the Cisco VEdge software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the Cisco VEdge software.

Delete a Software Image

To delete a software image from a SD-Routing device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Controller**, or **Cisco SD-WAN Manager**.
3. Choose one or more devices from which you want to delete a software image.
4. Click the **Delete Available Software**.

   The **Delete Available Software** dialog box opens.
5. Choose the software version to delete.
6. Click **Delete**.

View Log of Software Upgrade Activities

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.
2. Click the **Arrow** icon to see details of a task. Cisco SD-WAN Manager opens a status window displaying the status of the task and details of the device on which the task was performed.

Monitoring the Device Using Cisco SD-WAN Manager

The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all the monitoring components and services of a Cisco SD-Routing devices. You can establish the connection and monitor the device using the following options:

- SSH Terminal
- Ping
- Traceroute

Also, you can collect the system status information in a compressed *.tar* file. Cisco SD-WAN Manager can retrieve and download a *.tar* file from the device. After retrieving the file, you can delete the copy of the file on the device to free up the disk space.

When you enable the SD-Routing mode, this feature is enabled on the device and Cisco SD-WAN Manager by default.

Monitoring the Device Using SSH

To establish the connection and monitor the device using the SSH option, perform these steps:

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

Step 2 Choose a device from the list of devices that is displayed.

Step 3 For a single device, click **. . .** for the desired device and choose **SSH Terminal**.

(Or)

Step 4 From the Cisco SD-WAN Manager menu, choose **tools** > **SSH Terminal**.

Step 5 Enter the password twice (same as SD-Routing) in the terminal to establish the connection with the device.

Step 6 From the terminal, execute the **show commands** to monitor the device.

Pinging the Device

To ping the device, perform these steps:

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

Step 2 Choose a device from the list of devices that is displayed.

Step 3 For a single device, click **. . .** for the desired device and choose **Ping**.

Step 4 From the **Monitor** page, enter the destination IP address.

Step 5 Click **Ping**.

The results of the ping will be printed in the window below.

Tracing the Route

To establish the connection and monitor the device using the trace routing option, perform these steps:

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

Step 2 Choose a device from the list of devices that is displayed.

Step 3 For a single device, click **. . .** for the desired device and choose **Trace Route**.

Step 4 From the **Trace Route** page, enter the destination IP address.

Step 5 Click the **Start** button to trace the route.

Alarms and Events

When an even occurs on an individual device in the overlay network, the device reports it by sending a notification to Cisco SD-WAN Manager. Cisco SD-WAN Manager then filters the event notifications and correlates related events, and it consolidates major and critical events into alarms.

Use the Alarms screen to display detailed information about alarms generated by SD-Routing devices in the overlay network.

Monitoring the Alarms and Events

You can view alarms from the Cisco SD-WAN Manager dashboard by clicking the **Bell** icon at the top-left corner. The alarms are grouped into Active or Cleared. By default, alarms are displayed for the last 24 hours. Alternatively, follow these steps to view alarms from the **Alarms** screen in Cisco SD-WAN Manager.

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

Step 2 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.

The alarms are displayed in graphical and tabular formats.

Step 3 To view more details for a specific alarm, click **…** for the desired alarm, and then click **Alarm Details**.

The **Alarm Details** window opens and displays the probable cause of the alarm, impacted entities, and other details.

Admin-Tech Files

You can view the generated admin-tech files whenever the admin-tech files are available on a device.

You can view the list of generated admin-tech files and then decide which files to copy from your SD-Routing device to Cisco SD-WAN Manager. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco SD-WAN Manager, the device, or both.

Requesting the Admin-tech File Using Cisco SD-WAN Manager

An Admin-tech file is a collection of system status information used for troubleshooting a given issue. To request a Admin-tech file, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.

Step 2 For a single device, click **. . .** for the desired device and choose **Generate Admin Tech**.

Step 3 In the **Generate admin-tech File** window, limit the contents of the Admin-tech tar file if desired:

a) The **Include Logs** check box is checked by default. Uncheck this check box to omit any log files from the compressed tar file.
b) Check the **Include Cores** check box to include any core files.

Note The core files are stored in the *bootflash:/core* or *harddisk:/core* directory on the local device.

c) Check the **Include Tech** check box to include any files related to device processes (daemons), memory details and operations.

Step 4 Click **Generate**.

Cisco SD-WAN Manager creates the Admin-tech file. The file name format is *hostname-date-time-admin-tech.tar.gz*.

Step 5 To veiw the generated Admin-tech file, from the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands** > **Show Admin Tech List**.

Requesting the Admin-tech File Using CLI

To request a Admin-tech file using CLI, perform these steps:

Use the **request tech-support** command to generate the admin-tech file.

```
Device#request tech-support
21:03:46.447 UTC Thu Aug 10 2023 : Collecting 'show tech-support'...
21:04:51.880 UTC Thu Aug 10 2023 : 'show tech-support' collected successfully!
21:04:55.091 UTC Thu Aug 10 2023 : Collecting binary traces...
21:04:55.216 UTC Thu Aug 10 2023 : Binary traces collected successfully!
21:04:55.219 UTC Thu Aug 10 2023 : Collecting platform-dependent files...
21:05:43.467 UTC Thu Aug 10 2023 : Platform-dependent files collected successfully!
21:05:43.475 UTC Thu Aug 10 2023 : Generating tech-support bundle...
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle file
bootflash:core/1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz [size: 8648 KB]
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle generated successfully!

1HX-2017#
1HX-2017#dir bootflash:core
Directory of bootflash:/core/

1471682  -rw-               1  Aug 11 2023 04:26:51 +00:00  .callhome
45       -rw-           25429  Aug 10 2023 21:05:56 +00:00
1HX-2017_RP_0-debug_bundle_20230810-210346-UTC-info.txt
49       -rw-         8854997  Aug 10 2023 21:05:54 +00:00
1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz
1471685  drwx             4096  Mar 22 2021 20:03:54 +00:00  modules

29633794048 bytes total (16795193344 bytes free)
1HX-2017#
```

Monitoring the Real Time Data

To ping the device, perform these steps:

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

Step 2 Choose a device from the list of devices that is displayed.

Step 3 For a single device, click **...** for the desired device and choose **Real Time**.

Step 4 Select the category of data from the **Device Options** drop-down list.

The results will be diplayed.

Configuration Examples

This section provides the configuration exmaples.

Example: Enabling Control Connection on Cisco SD-WAN Manager

This example shows how to enable control connection on Cisco SD-WAN Manager:

```
(config) sd-routing
(config-sd-routing) system-ip  172.16.255.15
(config-sd-routing) organization-name viptela
(config-sd-routing) vbond ip 10.0.12.26
(config-sd-routing) site-id 500
(config-sd-routing) wan-interface GigabitEthernet2
```

Example: Verifying the Enable Control Connection

Use the **show platform software yang-management process state** command to check the connection status.

```
Device#show platform software yang-management process state
Confd Status: Started


Process              Status              State
------------------------------------------------------
nesd                 Running             Active
syncfd               Running             Active
ncsshd               Running             Not Applicable
dmiauthd             Running             Active
nginx                Running             Not Applicable
ndbmand              Running             Active
pubd                 Running             Active
```

Use the **show platform software yang-management process list r0 name vdaemon** command to check the vdaemon status.

```
Device#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
```

```
Kernel time      : 347183
Priority         : 20
Virtual bytes    : 405110784
Resident pages   : 12195
Resident limit   : 18446744073709551615
Minor page faults: 716496
Major page faults: 9130
```

Example: Installing the Root Certificate

This examples shows how to install the root certificate:

```
Device# request platform software sd-routing root-cert-chain install bootflash:root-ca.crt
```

Example: Verifying the Root Certificate Installation

Use the **show sd-routing local-properties summary** command to check the root certificate installation status.

```
Device#show sd-routing local-properties summary
personality                         vedge
sp-organization-name                vIPtela Inc Regression
organization-name                   vIPtela Inc Regression
root-ca-chain-status                Installed
root-ca-crl-status                  Not-Installed
```

```
Device#show sd-routing local-properties summary
certificate-status                  Installed
certificate-validity                Valid
certificate-not-valid-before        Apr 25 00:55:28 2023 GMT
certificate-not-valid-after         Apr 24 00:55:28 2024 GMT
….........
dns-name                            vbond
site-id                             100
tls-port                            0
system-ip                           172.16.255.11
chassis-num/unique-id               C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                          12345707
```

Troubleshooting

This section provides commands that can be used to troubleshoot the common issues while managing and monitoring the SD-Routing devices using Cisco SD-WAN Manager:

- **Show version**

Note The operating mode is included in **show version** command.

```
When sd-routing feature is enabled:
Device#show version | include mode
Router operating mode: Autonomous (SD-Routing)
Device#
```

```
When sd-routing feature is not enabled:
Device#show version | include mode
Router operating mode: Autonomous
Device#
```

- `show platform software yang-management process state`
- `show sd-routing system status`
- `show sd-routing connections summary`
- `show platform software process list r0 name vdaemon`
- `show sd-routing local-properties summary`
- `show sd-routing local-properties wan ipv4`
- `show sd-routing local-properties vbond`
- `show sd-routing connections history`

Feature Information for Managing SD-Routing Devices Using Cisco SD-WAN Manager

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for SD-Routing Devices Using Cisco SD-WAN Manager

Feature Name	Releases	Feature Information
Managing SD-Routing Devices Using Cisco SD-WAN Manager	Cisco IOS XE Release 17.12.1a	This feature allows you to perform management operations for SD-Routing devices using Cisco SD-WAN Manager. You can use a single network manage system (Cisco SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.