

SD-Routing: Onboard Routing Devices to Cisco SD-WAN Manager, Release 17.16.x

Overview

This document provides guidance to onboard the Cisco Routing devices into the enterprise SD-WAN infrastructure. These physical or virtual routing devices (also called autonomous devices) can be onboarded using one of the available methods - automated, bootstrap or manual. The document focuses on procedures to configure each of the available onboarding options, along with the use cases specific to device deployment using default pre-installed certificates or enterprise Root CA certificates.

Prerequisites

Before you begin onboarding the autonomous routing devices to the Cisco SD-WAN Manager, it is good to know the following.

Table 1: General Prerequisites

| What | Why |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An understanding of the SD-WAN architecture | Provides an understanding of the key players and the flow of information between these components. For more information about the SD-WAN architecture, see the <i>Cisco Catalyst SD-WAN Getting Started Guide</i> here https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html . |
| An understanding of Enterprise networks and the role of certificates | <p>Provides an understanding of how device identity is validated via certificates.</p> <p>There are different ways to accomplish the control component certificate signing and installation process:</p> <ul style="list-style-type: none"> • (Recommended): If your network uses the Cisco Public Key Infrastructure (PKI), you do not need to upload any certificate. For an understanding of PKI see https://www.cisco.com/c/en/us/tech/security-vpn/public-key-infrastructure-pki/index.html and the https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_comm_pki/configuration/15-mt/sec-pki-15-mt-book/sec-pki-overview.html guide. • If your network is an Enterprise network, then upload a Root CA. <p>For more information about enterprise certificates, see the https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html.</p> |

| What | Why |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The prerequisites for all onboarding options | <p>The Cisco Plug and Play(PnP) Connect server at http://software.cisco.com must have the Routing device added and associated with the VBOND controller profile. This action ensures that the device is in the SD-WAN Validator's allowed list of devices. The allowed list <i>provision file</i> can be downloaded from the PnP portal and uploaded to the SD-WAN Manager or synchronized with the SD-WAN Manager via the Sync Smart Account option. SD-WAN Manager later distributes this allowed list to the Validator.</p> <p>Software Routing devices deployed in virtual environment do not have chassis or serial number. For such devices, PnP server generates a unique serial number when the software device is added in the PnP portal.</p> <p>Refer to Add a Routing Device to Plug and Play Connect Portal , on page 6 to know more about how to add devices.</p> |
| An understanding of your specific deployment scenario | Helps to decide the best onboarding method for your requirement. based on whether you have new or existing devices. See Preferred Onboarding Options , on page 5. |

Table 2: Device-Specific Prerequisites

| | |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimum ReleaseVersion | <p>Routing Device - Cisco IOS XE 17.12.1a and should be in Install mode for booting the device.</p> <p>Cisco SD-WAN - 20.12.1</p> |
| Routing device settings | <ul style="list-style-type: none"> • You need to enable netconf-yang models for enabling DMI which is required for managing from Cisco SD-WAN Manager. • Device should be operating in autonomous mode before you onboard • Device must be configured to reach the Cisco SD-WAN Manager and the Cisco SD-WAN Validator over the WAN interface. The interface must be configured with a static IP address or through DHCP and must be in no shut state. |



| | |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing device details | <p>Needed during onboarding. The factory default routing device should be able to resolve FQDN devicehelper.cisco.com and reach the Cisco cloudhosted PnP Connect server to retrieve the vBond controller information, organization-name and enterprise root-ca certificates (if using enterprise root-ca certificates).</p> <ul style="list-style-type: none"> • Site ID • Organization-name • Cisco SD-WAN Validator information (IP address or FQDN Cisco SD-WAN Validator server) • Interface for connection to Cisco SD-WAN Manager (Physical, Sub-interface, and Loopback) • System IP: The system IP address provides a fixed location for the device in the network and is unique across all SD-routing devices in the network. The system IP is used as the device's loopback address in the Global VRF. This address cannot be used for another interface in Global VRF. |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Supported WAN Edge Devices

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

Table 3: 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 |

| Platforms | Automated | Bootstrap | Manual |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------|--------|
| Cisco 1000 Series Integrated Services Routers | | | |
| Cisco 1000 ISR  Note ISR1100-4G/6G and ISR1100X-4G/6G do not support SD-Routing mode. | Yes | Yes | Yes |
| Cisco Catalyst 8000V Series Edge Platforms | | | |
| Cisco Catalyst 8000V  Note Automated onboarding is applicable only for the hardware device. | Not applicable | 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 |
| 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 |
| Cisco Industrial Routers and Gateways | | | |
| ESR 6300 | Yes | Yes | Yes |
| IR1101 | Yes | Yes | Yes |
| IR1800 | Yes | Yes | Yes |
| IR8140H | Yes | Yes | Yes |

| Platforms | Automated | Bootstrap | Manual |
|---------------------------------------------|-----------|-----------|--------|
| IR8340 | Yes | Yes | Yes |
| Cisco 1100 Terminal Services Gateway | | | |
| C1100TGX-1N24P32A | Yes | Yes | Yes |
| C1100TG-1N24P32A | Yes | Yes | Yes |

Preferred Onboarding Options

Depending on your deployment scenario and the type of device, you can choose the best method for onboarding your device.

Table 4: Preferred Onboarding Method

| Device Type | Preferred Onboarding Option |
|-----------------------------------|----------------------------------------------------------------------|
| New Device | |
| <i>Hardware (Physical) Device</i> | Using PnP and Quick Connect |
| | Using Generic Bootstrap on the Cisco Catalyst SD-WAN Manager |
| <i>Software(Virtual) Device</i> | Using Device Specific Bootstrap on the Cisco Catalyst SD-WAN Manager |
| Existing Device | |
| <i>Hardware Device</i> | Manual Onboarding |
| | Bootstrap Onboarding |
| | One Touch Provisioning |
| <i>Software(Virtual) Device</i> | |
| | Manual Onboarding |
| | Chassis Number and Token CLI Onboarding |

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.
- Cisco SD-Routing devices can only have one control connection to Cisco SD-WAN Manager from an interface with reachability to the controllers.
- Cisco 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.

Onboard a New Hardware(Physical) Routing Device Using Automated Workflow

The automated Plug-and-Play (PnP) process provides a simple, secure procedure to discover, install and provision the Routing devices to join the SD-WAN network. This method of onboarding is supported for new hardware devices that are a part of new deployments.

To onboard the autonomous Routing devices using the automated workflow, perform these steps:

| Task | Description |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure the Plug and Play(PnP) Connect Portal with Routing device information | The PnP portal is populated with device information collected from the Smart Accounts and Virtual Accounts when ordering devices from Cisco Commerce Workplace (CCW). When new devices are onboarded other than CCW, you need to first add them to the PnP portal. |
| Add the autonomous Routing device to the Cisco SD-WAN Manager using Quick Connect workflow | Auto syncs the device information from Cisco PnP portal to SD-WAN Manager. |
| Complete onboarding the SD-Routing device | The routing device initiates and establishes secure connections with the SD-WAN Manager and SD-WAN Validator and joins the SD-WAN network. |
| Verify the onboarding status of the SD-Routing device | Verify the control connections. |

Add a Routing Device to Plug and Play Connect Portal

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

The Cisco PnP portal contains a list of devices that are associated with a given controller.

To add the devices to the PnP Connect portal, perform these steps:

Step 1 Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and log in to the **Plug and Play Connect Portal**.

Step 2 Under the **Controller Profiles** tab, click on **Add Profile** to create a profile with controller type as VBond.

Step 3 Enter the required profile settings in the **Add Controller Profile** window.

Step 4 If your overlay network is an Enterprise network, upload a Root CA and click **Next**.



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

Note

Step 5 Add the device to PnP Connect. In the **Identify Device** window enter the following:

- Serial Number
- Base PID
- (Optional) Certificate Serial Number


- Step 6** Next, choose the method to add the device. Choose one from the following options.
Choose from:
- **Import using a CSV file** (optional) - Do this if you have multiple devices to onboard.
 - **Enter Device info manually** (optional but recommended) - To do this you need to have the SD-Routing device specific information for Cisco PnP SA/VA. This can be obtained by entering the following CLI command on the SD-Routing device:
Router# show crypto pki certificate CISCO_IDEVID_SUDI
 - Add a device with the serial number from **show pnp udi** command or **show pnp version** command in PnP Connect.
- Step 7** Select the controller profile created earlier to associate the device with the validator (Cisco Catalyst SD-WAN Validator) controller profile.
- Step 8** Select the **Device Mode** as **AUTONOMOUS** for the device to operate in SD-Routing mode.

What's next

Add/Import/Sync Routing device to the Catalyst SD-WAN Manager using the Quick Connect workflow.

Add the Device in the Cisco SD-WAN Manager Using Quick Connect Workflow

To sync the Routing device information with the Cisco SD-WAN Manager, using the Quick Connect workflow, perform these steps:
The SD-Routing device must have been added to the PnP portal.

- Step 1** From the Cisco SD-WAN Manager menu, go to **Workflows > Quick Connect > Get Started**.
- Step 2** Add the Routing devices to the Cisco SD-WAN Manager by Sync Smart Account option.
-  **Note** Ensure that you have saved your smart account credentials on the Cisco Catalyst SD-WAN Manager. Go to **Administration > Settings > Smart Account Credentials** and enter the details. You can enable the Sync Smart Account only after saving the credentials.
- The device is now listed under the **Edge Devices**.
- Step 3** Select the device that you want to onboard and click **Next**.
- Step 4** In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
- Step 5** (Optional) Add a tag and click **Next**.
- Step 6** Review the device details and click **Onboard**.
The devices added in PnP Connect will be synced with Cisco SD-WAN Manager and sent to the Validator to be included in their allowed list of devices.
- Step 7** Verify the device is added, go to **Configuration > Devices > WAN Edge List**.
A list of SD-Routing devices in the network is displayed, showing detailed information about each router and the status as **Unreachable**.

What's next

What to do next:

Bring up the device and verify the connection.

Bring 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** Connect the SD-Routing device wan-interface to a DHCP enabled WAN link and power it on. Ensure that the device gets the IP address over DHCP on one of the interfaces other than the Gigabit Ethernet0 interface. Also, ensure that the device is reachable to devicehelper.cisco.com and the Cisco SD-WAN Validator.



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

Note

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

- Step 3** Verify the control connection status on the routing device. Enter the **show sd-routing system status**, **show sd-routing local-properties summary** and the **show sd-routing connections summary** command

Example:

```
Router#show sd-routing connections summary
```

| PEER | PEER | PEER | SITE | PEER | PEER | PRIV |
|----------------------|------------|--------|---------------|-------|------------|------------|
| TYPE | PROT | SYSTEM | IP | ID | PRIVATE | IP |
| 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 4** On the Catalyst SD-WAN Manager, navigate to **Configuration > Devices** to verify that the device status is shown as **In Sync** and **Reachable**.

Onboard a New Hardware(Physical) Routing Device Using Generic Bootstrap

The bootstrap file onboarding option involves adding the new hardware routing (physical) device information from the PnP portal to the Catalyst SD-WAN Manager using the Quick Connect workflow, and using the generic bootstrap file to onboard the device. Use this method in case of new deployments using new devices, where you don't have DHCP servers providing information. In such cases, the SD-WAN Manager can be used to generate a bootstrap file using which the device onboards as a SD-Routing device to the SD-WAN framework.

Ensure that your devices are added to the PnP portal. The Cisco PnP portal contains a list of devices that are associated with a given controller. Refer to [Add a Routing Device to Plug and Play Connect Portal](#), on page 6 on how to add a device to the PnP portal.

To onboard the new hardware device using the bootstrap option, perform these steps:

- Step 1** Sync your device inventory. On the SD-WAN Manager, go to **Workflows > Quick Connect** and click **Get Started**. Use one of the options to add the devices:
Choose from:

- **Log into your Smart Account** - (Preferred) Enter your credentials to add the device to SD-WAN Manager. The device information is synced from PnP Connect portal and is listed under **Configuration > Devices** page.

OR

- **Upload file with serial numbers** - Upload the .csv file containing the device information. You can gather this information by entering the CLI command on the Routing device.

```
Device# show crypto pki certificate CISCO_IDEVID_SUDI
```

A sample csv file is shown below.

| chassis number | product id | cert serial number | sudi serial | mode |
|----------------------|------------|--------------------|-------------|------------|
| ISR4461K9FDU1231M56W | ISR4461/K9 | 0215ZS7X | FDU1231M56W | autonomous |

The device is now listed under the **Edge Devices**.

- a. Select the device that you want to onboard and click **Next**.
- b. In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
- c. Review the device details and click **Onboard**. To verify the device that is added, go to **Configuration > Devices > WAN Edge List**. A list of routers in the network is displayed, showing detailed information about each router and the status as **Unreachable**.

Step 2 From the Cisco SD-WAN Manager menu, choose **Configuration > Devices** and select the device for which you want to generate the bootstrap.

Step 3 Click the **Export Bootstrap Configuration** dialog box, enter the **WAN Interface name** and select the checkbox for **SD-Routing** to generate the bootstrap file. The bootstrap file contains the organization name, Cisco SD-WAN validator IP, and root-ca certificates. For the enterprise network, it will have the enterprise root-ca- certificates.



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 Manager. Check the interface on the Routing device and ensure that it has connectivity to both.

Step 4 Download the generic .cfg bootstrap applicable for the hardware devices. Unzip the file and rename it as **ciscosdwan.cfg**.

Step 5 Copy the bootstrap file to the device internal bootflash as **ciscosdwan.cfg**. The downloaded bootstrap file is added as a user data field and brings up the device in SD-Routing mode and establishes the connection with the Cisco Catalyst SD-WAN Validator and Cisco SD-WAN Manager.

Step 6 Reload the device with **controller-mode reset** or **writer erase with reload** command to bring it to Day-0 state.

Step 7 Verify the control connection using these commands on the device:

Example:

```
Router# show sd-routing connections summary
```

```
Router# show sd-routing system status
```

```
Router# show sd-routing local-properties summary
```

Step 8 On the Catalyst SD-WAN Manager, navigate to **Configuration > Devices** to verify that the device status is shown as **In Sync** and **Reachable**.

Onboard a New Software (Virtual) Routing Device Using Device-Specific Bootstrap

The bootstrap file onboarding option involves adding the new software routing (virtual) device information from the PnP portal to the Catalyst SD-WAN Manager using the Quick Connect workflow, and using the device-specific bootstrap file to onboard the device. Use this method in case of new deployments using new devices, where you don't have DHCP servers providing information. In such cases, the Cisco SD-WAN Manager can be used to generate a bootstrap file using which the device onboards as a SD-Routing device to the SD-WAN framework.

Ensure that your devices are added to the PnP portal. The Cisco PnP portal contains a list of devices that are associated with a given controller. Refer to [Add a Routing Device to Plug and Play Connect Portal](#), on page 6 on how to add a device to the PnP portal.

- Install C8000v software on a virtual machine of your choice. For more information see [Installation Requirements for Installing C8000v on a Virtual Machine](#)
- Check the overlay network. If :
 - Overlay is Cisco PKI, Symantec/Digicert, no need to add and install the Root CA certificate.
 - Overlay is Enterprise, install the corresponding Root CA and signed certificate using the command.

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

You do not have to generate a Certificate Signing Request (CSR) and sign it. The CSR will be generated when you activate the device using the token.

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

Step 1 Sync your device inventory. On the SD-WAN Manager, go to **Workflows > Quick Connect** and click **Get Started**. Use one of the options to add the devices:

Choose from:

- **Log into your Smart Account** - (Preferred) Enter your credentials to add the device to SD-WAN Manager. The device information is synced from PnP Connect portal and is listed under **Configuration > Devices** page.
- OR
- **Upload file with serial numbers** - Upload the serial.viptela file downloaded from PnP Connect containing the device information(available under **Controller Profiles** and click **Download the Provisioning file** of PnP Connect portal). The device is now listed under the **Edge Devices**.
 - a. Select the device that you want to onboard and click **Next**.
 - b. In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
 - c. Review the device details and click **Onboard**. To verify the device that is added, go to **Configuration > Devices > WAN Edge List**. A list of routers in the network is displayed, showing detailed information about each router and the status as **Unreachable**.

Step 2 If you are using enterprise certificates, go to **Administration > Settings > Trust and Privacy > Controller Certificate Authorization** and select **Enterprise Root Certificate** and paste the enterprise root-cert. This ensures that you have the enterprise root-cert in the bootstrap file.

Step 3 Go to **Configuration > Devices** and select the device for which you want to generate the bootstrap.

Step 4 Click **...** at the right pane of the window and choose **Generate Bootstrap Configuration** and specify one or more valid ethernet interfaces. If enterprise certificates are being used, include the information in the provided field.



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

Note

Step 5 Click **OK** and download the .cfg file on the device. The following example shows a sample file type.

Example:

```
ciscosdwan_cloud_init.cfg
```

This .cfg file includes all the information to onboard the C8000v device on a hypervisor or a cloud platform such as AWS or Azure.

In the AWS EC2 console, upload the .cfg file or copy paste the contents of the file in the **User Data** field. If you are onboarding C8000v on Azure, copy paste the contents of the .cfg file in the **Custom Data** field. Proceed with the prompts displayed on the screen to complete the process of deploying C8000v on a cloud platform.

To onboard C8000v on a hypervisor, proceed with step 6.

Step 6 Convert the downloaded file to a consumable form for the virtual machine. Create a disk image from the file using the following command:

Example:

```
mkisofs -l -o /my/path/c8000v_config.iso ciscosdwan_cloud_init.cfg
```

Step 7 Mount the c8000v_config.iso as an additional disk during creation of the Cisco Catalyst 8000V virtual machine by using the following steps:

| Option | Description |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installing c8000v_config.iso file in KVM environment | <ol style="list-style-type: none">Set up the hypervisor using instructions in Creating a KVM Instance.After setting up the hypervisor, install the c8000v_config.iso file using instructions in Customizing Configuration Before Creating the VM. |
| Installing c8000v_config.iso file in VMWare ESXi environment | <ol style="list-style-type: none">Set up the hypervisor using instructions in Manually Creating the VM using .iso File. |

Step 8 Verify the control connection using these commands on the device:

Example:

```
Router# show sd-routing connections summary
```

```
Router# show sd-routing system status
```

```
Router# show sd-routing local-properties summary
```

Step 9 On the Catalyst SD-WAN Manager, navigate to **Configuration > Devices** to verify that the device status is shown as **In Sync** and **Reachable**.

Onboard an Existing Hardware(Physical) Routing Device Manually

This onboarding option involves manually adding the hardware routing device information from the PnP portal to the Catalyst SD-WAN Manager using the Quick Connect workflow and onboarding the routing device by applying additional configurations on the routing device. Use this method when the device is isolated, or the Cisco SD-WAN Manager instance is unable to connect with the Cisco PnP portal or you do not want to use the auto sync option which requires you to sync your Smart Account with Cisco SD-WAN Manager. You need to stop the PnP discovery and ensure that device has got startup configuration(or any configuration) and is not in Day-0 state.

- Ensure that your devices are added to the PnP portal. The Cisco PnP portal contains a list of devices that are associated with a given controller. Refer to [Add a Routing Device to Plug and Play Connect Portal](#) , on page 6 on how to add a device to the PnP portal.
- Check the overlay network. If :
 - Overlay is Ciscopki, Symantec/Digicert, no need to add install Root CA.
 - Overlay is Enterprise network, install the corresponding Root CA and signed certificates using the command.

Router# request platform software sd-routing root-cert-chain install bootflash:cacert.pem

To onboard the hardware Routing devices manually, perform these steps:

Step 1 Sync your device inventory. On the SD-WAN Manager, go to **Workflows > Quick Connect** and click **Get Started**. Use one of the options to add the devices:

Choose from:

- **Log into your Smart Account** - (Preferred) Enter your credentials to add the device to SD-WAN Manager. The device information is synced from PnP Connect portal and is listed under **Configuration > Devices** page.

OR

- **Upload file with serial numbers** - Upload the .csv file containing the device information. You can gather this information by entering the CLI command on the Routing device.

```
Device# show crypto pki certificate CISCO_IDEVID_SUDI
```

A sample csv file is shown below.

| chassis number | product id | cert serial number | sudi serial | mode |
|-----------------------|------------|--------------------|-------------|------------|
| ISR4461/K9FDU1231M56W | ISR4461/K9 | 0215ZS7X | FDU1231M56W | autonomous |

The device is now listed under the **Edge Devices**.

- Select the device that you want to onboard and click **Next**.
- In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
- Review the device details and click **Onboard**. To verify the device that is added, go to **Configuration > Devices > WAN Edge List**. A list of routers in the network is displayed, showing detailed information about each router and the status as **Unreachable**.

Step 2 Configure the minimum parameters on the Routing device to enable the control connection with the Cisco SD-WAN Manager.

Example:

```
router(config)# 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
```



Note Ensure that the interface is configured with a static IP address or through DHCP. It must have IP reachability to both the Cisco Catalyst SD-WAN Manager and Cisco Catalyst Validator. Also, the interface must be in **no shut** state.

Control connections are established between the routing device, validator and Catalyst SD-WAN Manager.

Step 3 Verify the control connection using these commands on the SD-Routing device:

Example:

```
Router# show platform software yang-management process state
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary
```

Step 4 On Cisco Catalyst SD-WAN Manager, navigate to **Configuration > Devices** and verify the device status is shown as **In Sync** and **Reachable**.

What's next

See Running Configuration - To do so, click (...) next to device and launch the menu.

Monitor Device - To do so, go to **Monitor > Device**, select device, click (...) to launch menu and see Alarms, Events, Troubleshoot etc.

Onboard an Existing Hardware(Physical) Routing Device Using Bootstrap

The bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive or from internal boot flash of a device that supports SD-Routing. When the device powers up, it adds the SD-Routing configuration to the existing configuration and comes up in the network without reloading the device.

You should stop the PnP discovery. The device must have either a start-up configuration or any configuration and the should not be in Day-0 state. Note that this method also works with Routing devices that had already been added to Cisco PnP SA/VA.

To onboard the existing hardware (physical) device using the bootstrap option, perform these steps:

Step 1 Sync your device inventory. On the SD-WAN Manager, go to **Workflows > Quick Connect** and click **Get Started**. Use one of the options to add the devices:

Choose from:

- **Log into your Smart Account** - (Preferred) Enter your credentials to add the device to SD-WAN Manager. The device information is synced from PnP Connect portal and is listed under **Configuration > Devices** page.

OR

- **Upload file with serial numbers** - Upload the .csv file containing the device information. You can gather this information by entering the CLI command on the Routing device.

```
Device# show crypto pki certificate CISCO_IDEVID_SUDI
```

A sample csv file is shown below.

| chassis number | product id | cert serial number | sudi serial | mode |
|----------------------|------------|--------------------|-------------|------------|
| ISR4461K9FDU1231M56W | ISR4461/K9 | 0215ZS7X | FDU1231M56W | autonomous |

The device is now listed under the **Edge Devices**.

- Select the device that you want to onboard and click **Next**.
- In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
- Review the device details and click **Onboard**. To verify the device that is added, go to **Configuration > Devices > WAN Edge List**. A list of routers in the network is displayed, showing detailed information about each router and the status as **Unreachable**.

Step 2 From the Cisco SD-WAN Manager menu, choose **Configuration > Devices** and select the device for which you want to generate the bootstrap.

Step 3 Click the **Export Bootstrap Configuration** dialog box, enter the **WAN Interface name** to generate the bootstrap file. The bootstrap file contains the organization name, Cisco SD-WAN Validator IP, and Root-CA certificates. For the enterprise network, it will have the enterprise Root-CA certificates.



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. Check the interface on the Routing device and ensure that it has connectivity to both.

Step 4 Download the generic .cfg bootstrap applicable for the hardware devices. Unzip the file and rename it as **ciscosdwan.cfg**.

Step 5 Copy the bootstrap file to the device internal bootflash as **ciscosdwan.cfg**.

Step 6 Enter the **sd-routing bootstrap load bootflash:ciscosdwan.cfg** command on the Routing device.

Example:

```
Router# sd-routing bootstrap load bootflash:ciscosdwan.cfg
Located the file. Beginning to extract the data
Extraction summary
-Organization name - "testb2"
-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
```

This brings up the device in SD-Routing mode and establishes the connection with the Cisco Catalyst SD-WAN Validator and Cisco SD-WAN Manager.

Step 7 Verify the control connection using these commands on the device:

Example:

```
Router# show sd-routing connections summary

Router# show sd-routing system status

Router# show sd-routing local-properties summary
```

Step 8 On the Catalyst SD-WAN Manager, navigate to **Configuration > Devices** to verify that the device status is shown as **In Sync** and **Reachable**. It also shows up on **Monitor > Device** as a SD-Routing device.

Onboard an Existing Hardware(Physical) Routing Device Using One Touch Provisioning

This task provides instructions for onboarding the Routing devices to the Catalyst SD-WAN Manager using One Touch Provisioning. One Touch Provisioning eliminates the need to add the Routing device to Cisco PnP SA/VA and to sync or upload the device list to Catalyst SD-WAN Manager prior to onboarding the device. Use this method if you have large network with a number of existing devices. Ensure that you stop the PnP discovery before you start onboarding the devices.

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

Step 1 On the SD-Routing device to be onboarded, enter the following commands.

Example:

```
Router(config)# netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org.Name%"
  site-id %id%
  system-ip %system ip%
  vbond name <FQDN> or vbond ip <ipaddress>
  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
```

This action initiates the communication with the Cisco Catalyst SD-WAN Validator and the device is added to the **Cisco Catalyst SD-WAN Manager > Devices > Unclaimed WAN Edges** list.

- Step 2** On the Cisco Catalyst SD-WAN Manager, navigate to **Configuration > Devices > Unclaimed WAN Edges** page, verify the device serial number and claim the SD-Routing device by checking the **Validate the uploaded vEdge List and send to controllers** check box.
This moves the device from the **Unclaimed WAN Edges** category to the **WAN Edges List** category and lets the SD-Routing device establish the control connection with the Catalyst SD-WAN Manager and complete the onboarding process.
- Step 3** Verify the control connection to the Cisco SD- WAN Manager by using these commands on the SD-Routing device:
- Example:**
- ```
Router# show sd-routing connections summary
```
- ```
Router# show sd-routing system status
```
- ```
Router# show sd-routing local-properties summary
```
- ```
Router# show sd-routing connection history
```
- Step 4** On the Catalyst SD-WAN Manager, navigate to **Configuration > Devices** to verify that the device status is shown as **In Sync** and **Reachable**.

Onboard an Existing Software(Virtual) Routing Device Manually

This onboarding option involves manually adding the software(virtual) routing device information from the PnP portal to the Catalyst SD-WAN Manager using the Quick Connect workflow and onboarding the routing device by applying additional configurations on the routing device.

Ensure that your devices are added to the PnP portal. The Cisco PnP portal contains a list of devices that are associated with a given controller. Refer to [Add a Routing Device to Plug and Play Connect Portal , on page 6](#) on how to add a device to the PnP portal. PnP discovery for this device should be stopped. The device should have startup configurations, and not be in Day-0 state.

To onboard the existing software Routing devices manually, perform these steps:

- Step 1** Sync your device inventory. On the SD-WAN Manager, go to **Workflows > Quick Connect** and click **Get Started**. Use one of the options to add the devices:
- Choose from:**
- **Log into your Smart Account** - (Preferred) Enter your credentials to add the device to SD-WAN Manager. The device information is synced from PnP Connect portal and is listed under **Configuration > Devices** page.
- OR
- **Upload file with serial numbers** - Upload the serial.viptela file downloaded from PnP Connect containing the device information(available under **Controller Profiles** and click **Download the Provisioning file** of PnP Connect portal). The device is now listed under the **Edge Devices**.
 - a. Select the device that you want to onboard and click **Next**.
 - b. In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
 - c. Review the device details and click **Onboard**. To verify the device that is added, go to **Configuration > Devices > WAN Edge List**. A list of routers in the network is displayed, showing detailed information about each router and the status as **Unreachable**.
- Step 2** On the routing device, configure the minimum parameters to enable control connection to Cisco SD-WAN Manager.

Example:

```
Router(config)# 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
```

- Ensure that the interface is configured with a static IP address or through DHCP. It must have IP reachability to both the Catalyst SD-WAN Manager and Validator. Also, the interface must be in **no shut** state.
- Configure either Validator IP or Validator Name.
- Configure the System-IP, Site-ID, Organization-Name and WAN-Interface.

Step 3 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 4 Cisco devices are loaded with PKI and Symantec root-certificates by default. If your overlay network is for an Enterprise, you need to install the Enterprise Root Certificate. Copy the root certificate from the Certificate Authority (CA) to Cisco 8000v. Enter the following commands. **scp** root-ca-chain.crt **cisco@<c8kv>:root-ca-chain.crt** and the **request platform software controller-managed root-cert-chain install** <path-to-root-cert> command.

Example:

```
Router# scp root-ca-chain.crt cisco@<c8kv>:root-ca-chain.crt
```

Example:

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

Step 5

Install the client enterprise certificates.

- a) Generate a Certificate Signed Request (CSR) for the device using the **request platform software sd-routing csr upload bootflash: tmp_cert_dir/C8kCsrFile.csr** command . You can specify any name for the folder that is created within the *tmp_cert_dir/* directory.
- b) Copy the generated CSR file from the c8k device to the directory where you have the Enterprise CA. You can sign the certificate using the root key and root CA certificate and generate the pem/crt certificate file.
 - In Enterprise CA : `scp cisco@<c8kv ip>:tmp_cert_dir/C8kCsrFile.csr`
 - `openssl x509 -req -in C8kCsrFile.csr -CA root-ca-chain.crt -CAkey rootCA.key -CAcreateserial -out C8kCsrFile.crt -days 3650 -sha256`
- c) Copy the generated crt file signed to c8000v device. In Enterprise CA: `scp C8kCsrFile.crt cisco@<c8kv ip>:C8kCsrFile.crt`
- d) Install the copied certificate on the device with **request platform software sd-routing certificate install bootflash:C8kCsrFile.crt** command.

Step 6

Verify the installation status of the certificates.

Example:

```
Router# 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 7

When you install the client certificate using the CLI, or if you had to redo the CSR generation and certificate installation due to any reason, ensure that you add the device information to the Cisco SD-WAN Manager for it to start control connections with the Cisco SD-WAN Manager . The steps are outlined below.

- a) Get the chassis number and serial number. To get the chassis number and serial number, use the **show 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 SD-WAN Manager and SD-WAN Validator.

Step 8

Verify the control connection status on the SD-Routing device.

Example:

```
Router#show sd-routing connections summary
```

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

Step 9 On Cisco Catalyst SD-WAN Manager, navigate to **Configuration > Devices** and verify the device status is shown as **In Sync** and **Reachable**.

Onboard an Existing Software(Virtual) Routing Device by Activating the Chassis Using the Token

This onboarding option involves adding the virtual routing device information from the PnP portal to the Catalyst SD-WAN Manager using the Quick Connect workflow (either SyncSmart or serial.viptela file) and onboarding the routing device by activating the token.



Note

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

- Ensure that you have saved your smart account credentials on the Cisco Catalyst SD-WAN Manager. You can do this on the Cisco Catalyst SD-WAN Manager by going to **Administration > Settings > Smart Account Credentials**. This will be used later to sync your Smart Account or Virtual account information in Cisco SD-WAN Manager.
- Check the overlay network. If :
 - Overlay is Ciscopki, Symantec/Digicert, no need to add and install the Root CA certificate.
 - Overlay is Enterprise, install the corresponding Root CA and signed certificate using the command.

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

You do not have to generate a Certificate Signing Request (CSR) and sign it. The CSR will be generated when you activate the device using the token.

To onboard the device by activating the chassis number, perform these steps:

Step 1 Sync your device inventory. On the SD-WAN Manager, go to **Workflows > Quick Connect** and click **Get Started**. Use one of the options to add the devices:

Choose from:

- **Log into your Smart Account** - (Preferred) Enter your credentials to add the device to SD-WAN Manager. The device information is synced from PnP Connect portal and is listed under **Configuration > Devices** page.
- OR
- **Upload file with serial numbers** - Upload the serial.viptela file downloaded from PnP Connect containing the device information(available under **Controller Profiles** and click **Download the Provisioning file** of PnP Connect portal). The device is now listed under the **Edge Devices**.
 - a. Select the device that you want to onboard and click **Next**.

- b. In the **Add and Review Device Configuration** dialog box, enter the Site-ID, System-IP (mandatory), Hostname, and click **Apply**.
- c. Review the device details and click **Onboard**. To verify the device that is added, go to **Configuration > Devices > WAN Edge List**. A list of routers in the network is displayed, showing detailed information about each router and the status as **Unreachable**.

Step 2 On the Routing device, run the following commands to apply the minimum configuration.

Example:

```
Router(config)# 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 3 Go to 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 4 To override the chassis number that is generated by the virtual device, run the CLI command on the virtual Routing device.

Example:

```
request platform software sd-routing activate chassis newly uploaded chassis id from vmanage
token token generated by SD-WAN Manager
```

Step 5 Verify the control connection status on the Routing 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
```

Step 6 On the Catalyst SD-WAN Manager, navigate to **Configuration > Devices** to verify that the SD-Routing device status is shown as **In Sync** and **Reachable**.

Troubleshoot Onboarding Issues

The following lists the common problems and resolution related to onboarding routing devices. If your solution is not listed here, we recommend that you raise a support ticket at [Cisco Support](#).

Mandatory checks on your device

Possible Cause sd-routing feature is not enabled

Solution Verify device operating mode

```
Router#show version | include mode
cisco ASR1002-HX (2KH) processor (revision 2KH) with 6756077K/6147K bytes of memory.
Processor board ID FXS2304Q345
Router operating mode: Autonomous (SD-Routing)
Crypto Hardware Module present
8 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
29401087K bytes of eUSB flash at bootflash:.
```

Solution Verify if confd is started.

```
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 |

Solution Verify if vdaemon is started.

```
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
```

Solution Verify using show commands

```
Router#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

certificate-status          Installed
certificate-validity        Valid
certificate-not-valid-before May  8 17:49:38 2023 GMT
certificate-not-valid-after  May  7 17:49:38 2024 GMT

enterprise-cert-status     Not Applicable
enterprise-cert-validity   Not Applicable
enterprise-cert-not-valid-before Not Applicable
enterprise-cert-not-valid-after Not Applicable
dns-name                   vbond
```

```

site-id 100
tls-port 0
system-ip 172.16.255.11
chassis-num/unique-id C8K-7d921537-5402-4c3c-a3b5-a273dafc44d9
serial-num 12345707
subject-serial-num N/A
enterprise-serial-num Not Applicable
token Invalid
keygen-interval 0:02:00:00
retry-interval 0:00:00:19
no-activity-exp-interval 0:00:00:20
dns-cache-ttl 0:00:02:00
port-hopped FALSE
time-since-last-port-hop 0:00:00:00
embargo-check success
number-vbond-peers 2
number-active-wan-interfaces 1

```

wan-interface and IP is not reachable

Possible Cause The wan-interface does not have a valid IP address.

Solution Verify wan-interface state and IP. Use the command

```

Router#show sd-routing local-properties wan ipv4

```

| INTERFACE | PUBLIC IPv4 | PUBLIC PORT | PRIVATE IPv4 | PRIVATE PORT | STATE |
|------------------|-------------|-------------|--------------|--------------|-------|
| GigabitEthernet2 | 10.0.5.11 | 12386 | 10.0.5.11 | 12386 | up |

Solution Ensure the wan-interface has a valid IP address and is in UP state.

Cisco Validator related issues

Cannot find Cisco Validator(vBond) information

Possible Cause The routing device is not associated with the Cisco Validator (vBond).

Solution Verify Cisco Validator(vBond) information

```

Router#show sd-routing local-properties vbond

```

| INDEX | IP | PORT |
|-------|---------------|-------|
| 0 | 10.0.12.26 | 12346 |
| 1 | 2001:a0:c::1a | 12346 |

Solution Ensure that the sd-routing device is connected to atleast one Validator.

Troubleshoot control connection issues

Routing device unable to connect to SD-WAN Manager after onboarding

Solution Use the following commands to check the connection status on the routing device.

```

Router#show sd-routing connections ?
detail  Display connections in detail
history Control connections history
summary Display connections summary

```

Problem sd-routing connections summary command is empty

Possible Cause Possibly no connection to SD-WAN Manager

Solution Use the following command to check the connection status on the routing device.

Solution If there are no active connections , there will be no output from the CLI

```
Router#show sd-routing connections summary
Router#
```

Solution If there are active connections, the view below indicates that.

```
Router#show sd-routing connections summary
```

| PEER TYPE | PEER PROT | PEER SYSTEM IP | SITE ID | PEER PRIVATE IP | PEER PRIV PORT | PEER PUBLIC IP | PEER PUB PORT | STATE | UPTIME |
|-----------|-----------|----------------|---------|-----------------|----------------|----------------|---------------|-------|------------|
| vmanage | dtls | 172.16.255.22 | 200 | 10.0.12.22 | 12446 | 10.0.12.22 | 12446 | up | 0:00:14:58 |

Solution Use the following command to check the connection status on the routing device.

```
Router# sh sd-routing connections history
```

| PEER TYPE | PEER LOCAL PROTOCOL | PEER SYSTEM IP | PEER REMOTE IP | PEER SITE REPEAT | PEER PRIVATE IP | PEER PRIVATE PORT | PEER PUBLIC IP | PEER PUBLIC PORT | STATE |
|-----------|---------------------|----------------|----------------|------------------|--------------------------|-------------------|----------------|------------------|-------|
| vmanage | dtls | 172.16.255.22 | 200 | 200 | 10.0.12.22 | 12446 | 10.0.12.22 | 12446 | |
| tear_down | | DISTLOC | NOERR | 0 | 2023-04-26T17:08:13+0000 | | | | |
| vbond | dtls | 0.0.0.0 | 0 | 0 | 2001:a0:c::1a | 12346 | 2001:a0:c::1a | 12346 | |
| connect | | DCONFFAIL | NOERR | 18 | 2023-04-25T01:04:08+0000 | | | | |
| vbond | dtls | 0.0.0.0 | 0 | 0 | 10.0.12.26 | 12346 | 10.0.12.26 | 12346 | |
| connect | | DCONFFAIL | NOERR | 8 | 2023-04-25T00:59:09+0000 | | | | |

Problem show sd-routing connections history command shows no output

Possible Cause Possibly no connection with Validator

Solution Use ping vbond command on routing device and verify reachability to Validator

```
Router#ping vbond
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:A0:C::1A, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/30 ms
Router#
```

DTLS Connection Failure (DCONFAIL)

This is one of the common issues of control connectivity that does not come up. Probable causes include a firewall or some other connectivity issues.

Possible Cause It could be that some or all packets are dropped/filtered somewhere. The example with larger ones is given in tcpdump results here.

- **Possible Cause** The next hop (NH) router is not reachable.
- **Possible Cause** The default gateway is not installed in the Routing Information Base (RIB).
- **Possible Cause** The Datagram Transport Layer Security (DTLS) port is not open in the controllers.

Solution Check ARP table for Default GW

```
Router# show arp
```

Solution Ping default GW

```
ping <...>
```

Solution Ping Google DNS

```
ping 8.8.8.8
```

Solution Ping vBond if ICMP is allowed on vBond

```
ping <vBond IP>
```

Solution Traceroute to vBond DNS

```
traceroute <...>
```

Board-ID not Initialized (BIDNTPR)

This is one of the common issues of control connectivity that does not come up. Probable causes include a firewall or some other connectivity issues.

Possible Cause Indicates that the routing device chassis-num/unique-id/serial number is rejected by the Validator

- **Possible Cause** The next hop (NH) router is not reachable.
- **Possible Cause** The default gateway is not installed in the Routing Information Base (RIB).
- **Possible Cause** The Datagram Transport Layer Security (DTLS) port is not open in the controllers.

Solution Check routing device serial number

```
Router#show sd-routing certificate serial
Chassis number: C8K-b596f134-0fa6-445f-9275-23f76ba90de0 serial number: 12345707 Subject S/N: N/A
```

Solution Ensure that this information is present in the list of valid routing devices for Cisco Validator.

```
vBond# show orchestrator valid-vedges
HARDWARE
```

| INSTALLED | SUBJECT | | | | |
|------------------------------------------|---------------|-----|----------|------------------------|--|
| SERIAL | SERIAL | | | | |
| CHASSIS NUMBER | SERIAL NUMBER | | VALIDITY | ORG | |
| NUMBER | NUMBER | | | | |
| ----- | | | | | |
| C8K-AA079CA1-C141-4AC6-9B76-05864005F94E | 12345707 | | valid | vIPtela Inc Regression | |
| N/A | N/A | N/A | | | |

Solution If an entry does not exist for the Routing device, ensure that you have

- **Solution** Added the routing device to the Smart Account
- **Solution** Uploaded the information to the SD-WAN Manager
- **Solution** Pushed this information to the Validator through **Configuration > Certificates > Send to Controllers**

Solution If it does exist, check for duplicate entries in the valid vEdge table and engage the Cisco Technical Assistance Center (TAC) to troubleshoot this further.

Serial Number(s) not Present (CRTREJSER, BIDNTRFD)

Indicates that the routing device chassis-num/unique-id/serial number is rejected by the Validator and the control connections fail.

Possible Cause Mismatch of information between the device and the controller

- **Solution** Verify the chassis-id/serial-num on the routing device. Use the `Router#show sd-routing local-properties summary` command to get the information and verify it in Validator with `vBond#show orchestrator valid-vedges` command.
- **Solution** If there is a mismatch, verify the correct information and upload to Smart Account or SD-WAN Manager

- **Solution** Verify that the **Organization Name** used by the device and controller is the same

Certificate related issues

Indicates that the routing device chassis-num/unique-id/serial number is rejected by the Validator and the control connections fail.

Possible Cause Mismatch of information between the device and the controller

Solution Use the following commands to view the certificates and identify the issues

```
Router#show sd-routing certificate installed
Router#show sd-routing certificate root-ca-cert
Router#show sd-routing certificate serial
Router#show logging process vdaemon internal
```

Debugging Control Connection Issues using Logs

Solution Use the following commands to view the vdaemon btrace logs and identify the issues

```
Router#show logging process vdaemon internal
Logging display requested on 2023/05/09 14:38:32 (UTC) for Hostname: [vm1], Model: [C8000V], Version: [17.13.01],
SN: [9HP3SG7HKUU], MD_SN: [SSI130300YK]
```

```
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Unified Decoder Library Init .. DONE
Found 1 UTF Streams
```

```
2023/05/09 14:29:18.917119471 {vdaemon_R0-0}{255}: [vdaemon-cert] [18612]: (note): Validating certificate..
ou_check enabled
2023/05/09 14:29:18.917189711 {vdaemon_R0-0}{255}: [bss] [18612]: (note): not found
"/C=US/CN=b6ebad1f-43b6-4900-b355-e699449c84ac/O=Cisco Systems":307542112 at idx -1
2023/05/09 14:29:18.917387747 {vdaemon_R0-0}{255}: [bss] [18612]: (note): x509_verify_cert Success crl_loaded
0
2023/05/09 14:29:18.993555137 {vdaemon_R0-0}{255}: [vdaemon-cert] [18612]: (note): Validating certificate..
ou_check enabled
2023/05/09 14:29:18.993572400 {vdaemon_R0-0}{255}: [bss] [18612]: (note): not found
"/C=US/CN=b6ebad1f-43b6-4900-b355-e699449c84ac/O=Cisco Systems":307542112 at idx -1
```

Request Tech Support

You can use **request tech-support** command on the routing device to generate a tar file containing logs, core and show command output.

```
Router#request tech-support
11:51:06.396 UTC Thu Jul 20 2023 : Collecting 'show tech-support'...
11:51:42.549 UTC Thu Jul 20 2023 : 'show tech-support' collected successfully!
11:51:43.798 UTC Thu Jul 20 2023 : Collecting binary traces...
11:51:43.965 UTC Thu Jul 20 2023 : Binary traces collected successfully!
11:51:43.967 UTC Thu Jul 20 2023 : Collecting platform-dependent files...
11:52:39.007 UTC Thu Jul 20 2023 : Platform-dependent files collected successfully!
11:52:39.013 UTC Thu Jul 20 2023 : Generating tech-support bundle...
11:52:46.873 UTC Thu Jul 20 2023 : Tech-support bundle file
bootflash:core/vml-debug_bundle_20230720-115143-UTC.tar.gz [size: 22358 KB]
11:52:46.873 UTC Thu Jul 20 2023 : Tech-support bundle generated successfully!

Router#dir bootflash:/core
Directory of bootflash:/core/

186      -rw-                10849   Jul 20 2023 11:52:46 +00:00  vml-debug_bundle_20230720-115143-UTC-info.txt
192      -rw-                22893633  Jul 20 2023 11:52:44 +00:00  vml-debug_bundle_20230720-115143-UTC.tar.gz
```

38 drwx 4096 Jul 18 2023 20:33:36 +00:00 modules

5173313536 bytes total (3922272256 bytes free)

vm1#



Note

The *.txt file contains the listing of all the files bundled into the tar.gz
