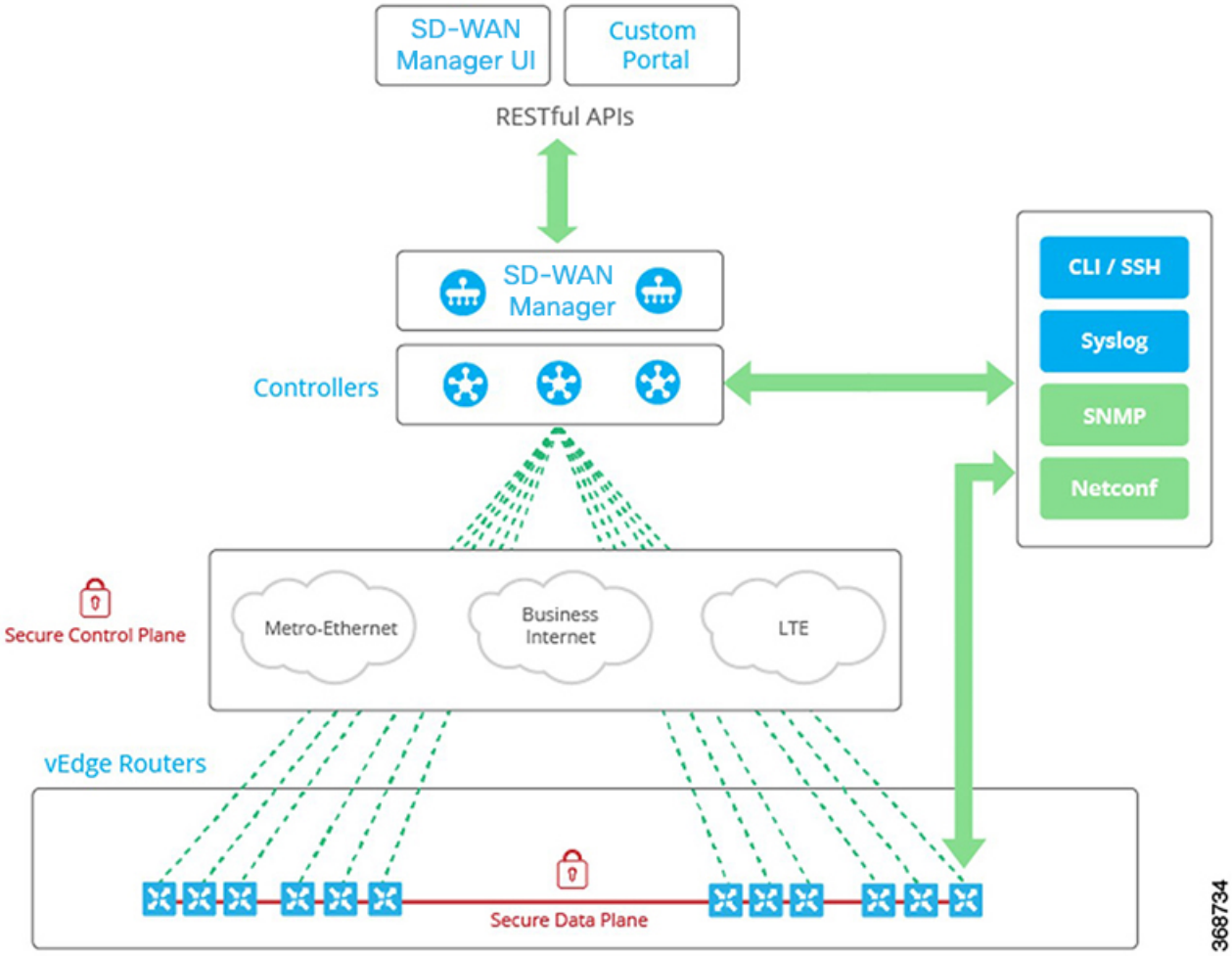
Appendix: Cisco Catalyst SD-WAN Manager How-Tos

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

RESTful API for Cisco Catalyst SD-WAN Manager

The Cisco SD-WAN Manager supports RESTful (Representational State Transfer) API, which provides calls for retrieving real-time and static information about the Cisco Catalyst SD-WAN overlay network and the devices in the network and for uploading device configuration templates and other configuration-related information. Using the RESTful API, you can design a custom portal for interacting with Cisco SD-WAN Manager.



The Cisco SD-WAN Manager API documentation is provided as part of the Cisco SD-WAN Manager software, at the URL https://*vmanage-ip-address*/apidocs. (More accurately, the full URL includes the Cisco SD-WAN Manager port number, https://*vmanage-ip-address*:8443/apidocs.) *vmanage-ip-address* is the IP address of the Cisco SD-WAN Manager server.

API calls are provided for the following categories of operations:

- Certificate Management
- Configuration
- Device and Device Inventory
- Monitoring
- Real-Time Monitoring
- Troubleshooting Tools

NAT configuration using REST APIs is not supported.

Note Starting from Cisco SD-WAN Release 20.6.1, Cisco SD-WAN Manager supports below API limits:

- API Rate-limit: 100/second
- Bulk API Rate-limit: 48/minute

Real-time monitoring of APIs is CPU intensive and should be used for troubleshooting purposes only. They should not be used continuously for active monitoring of the devices.

For each group of API calls, click **Show/Hide** to list the individual calls and the URL for each call. Each call shows its response class, required parameters, and response messages (status codes).

Click **Try It Out**, to display the request URL for each API call and the format of the response body. The request URL consists of the Cisco SD-WAN Manager's URL, followed by /dataservice. For example, https://10.0.1.32:8443/dataservice/device/interface/statistics/ge0/0?deviceId=172.16.255.11

Below are a few examples of the URLs to use for API calls:

Table 1:

Requested Information	API Call
List all network devices	dataservice/device
Health status of hardware device components, such as CPU, memory, fan, and power	dataservice/device/hardware/environment?deviceId=*system-ip-address*
Status of a device's transport interfaces	dataservice/device/interface?deviceId=*system-ip-address*&port-type=transport
Interface statistics, errors, and packet drops	dataservice/device/interface?deviceId=*system-ip-address*
DTLS/TLS control connection status	dataservice/device/control/connections?deviceId=*system-ip-address*
OMP peering	dataservice/device/omp/peers?deviceId=*system-ip-address*
BGP peering on the service side	dataservice/device/bgp/neighbors?deviceId=*system-ip-address*

Replace a vEdge Router

This section describes how to replace a vEdge router at a particular location. You might do this when a vEdge router has failed completely or when a component in a router, such as one of the power supplies, has failed, and you want to replace the entire router.

At a high level, to replace one vEdge router with another, you simply copy the configuration from the router you are removing to the new router and then put the new router into the network.

Before you can replace the vEdge router in Cisco SD-WAN Manager, Cisco SD-WAN Manager must have learned the chassis number and serial number of the replacement vEdge router.

- If the replacement vEdge router is a router that you have previously received, such as a router that part of your spares inventory, Cisco SD-WAN Manager will have already learned the router's chassis and serial number when you previously uploaded the serial number file to Cisco SD-WAN Manager.
- If you initiated an RMA process and have received a new router as a replacement, you need to upload the updated version of the authorized vEdge serial number file to Cisco SD-WAN Manager.

To replace a failed router using Cisco SD-WAN Manager, perform the following steps:

1. Copy the configuration from the failed router to the replacement router.
2. Invalidate the failed router. Invalidating a router deactivates its certificate and thus removes it from the overlay network.
3. Validate the replacement router, to activate its certificate.

The new router is a complete replacement for the failed router, its configuration is identical to that of the failed router. (Remember, though, that each router has a unique chassis number and a unique serial number in its certificate.) After you copy the configuration from the failed router to the replacement, both routers have the same configurations, including the same IP address. Two routers with the same IP address cannot be present in the network at the same time, one router must be in valid state on Cisco SD-WAN Manager and the other must be in invalid state—or both routers must be in invalid state.

Before You Begin

Ensure that you have uploaded the authorized serial number file to Cisco SD-WAN Manager.

Copy the Configuration from the Failed to the Replacement Router

From Cisco SD-WAN Manager, you copy the configuration from the failed vEdge router to the replacement router.

The vEdge router that you are copying the configuration from can be a device that is active in the overlay network (that is, it is in a valid state) or it can be one that is inactive (that is, it is in invalid state). For example, if you are replacing a router in which one of the two power supplies has failed, the router might still be active in the network, but if you are replacing one that has failed completely, you might have already marked it as invalid to remove it from the network.

The vEdge router that you are copying the configuration to must be in invalid state.

To view the state of a vEdge router or to change the validity state, see Validate or Invalidate a vEdge Router.

To copy the configuration from the failed router to the replacement router:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. For the failed router, click **...** and choose **Copy Configuration**.
3. In the **Copy Configuration** window, choose the replacement router.
4. Click **Update**.

Remove the Failed Router

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. For the failed router, in the **Validate** column, click **Invalid**.
3. Click **OK** to confirm invalidation of the device.
4. Click **Send to Controllers**.

Add the Replacement Router

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. For the replacement router, in the **Validate** column, click **Valid**.
3. Click **OK** to confirm validation of the device.
4. Click **Send to Controllers**.

If you attempt to validate a router that has the same IP address as another router in the network, an error message is displayed, and the validation process is terminated.

Release Information

Introduced in Cisco SD-WAN Manager in Release 15.4.

Replace a Cisco IOS XE Catalyst SD-WAN Device

You might replace a Cisco IOS XE Catalyst SD-WAN device if the device has failed completely or when a component of the device, such as one of the power supplies, has failed.

In general terms, to replace one Cisco IOS XE Catalyst SD-WAN device with another, copy the configuration from the device that you are removing to the new device and then add the new device into the network.

A. Copy the configuration from the device that you are replacing

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. In the list of devices, locate the device to be replaced. In the row of the device, click **…** and choose **Running Configuration**.

Note If Cisco SD-WAN Manager cannot reach the device, skip to step 4 for instructions on logging in to the device directly to copy the configuration information.

3. Copy the text of the configuration and paste it into a text editor.

   The configuration information is useful especially if you choose the manual deployment method for onboarding the new replacement device.

4. If the device is not reachable by Cisco SD-WAN Manager, log in to the device directly and use the following commands on the device to display the configuration information. Copy the configuration information from the output.

- Display the running configuration and save the output to a text file.

```
show running-config | redirect bootflash:sdwan/ios.cli
```

- Display the SD-WAN running configuration and save the output to a text file.

```
show sdwan running-config | redirect bootflash:sdwan/sdwan.cli
```

B. Remove the device from the overlay network

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. In the list of devices, locate the device to be replaced. In the row of the device, in the **Validate** column, click **Invalid**, then **OK**.

Note This step causes any control connections to the device to be lost.

3. Click **Send to Controllers**.
4. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
5. In the list of devices, locate the device to be replaced. In the row of the device, click **…** and choose **Delete WAN Edge**.

C. Add the replacement device to the Cisco SD-WAN Manager inventory

1. Obtain the chassis number and serial number of the replacement device.

Note You can use the **show sdwan certificate serial** command on the device to display this information.

2. Add the new device to the inventory using one of the methods described in the Cisco Catalyst SD-WAN Getting Started Guide.

Note The methods for adding a new device to the inventory are relevant to onboarding devices in general. They are not unique to replacing a device.

D. Apply a device template to the new device, using the same device template that was applied to the device that is being replaced

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. In the row for the template that was used for the device being replaced, click **…** and choose **Export CSV**. The CSV file shows the parameters for each device to which the template is attached.
3. Review the exported CSV file.
   - If the new device is identical to the device being replaced, you do not need to update any of the parameters in the CSV file.

- If the new device is not identical to the device being replaced, then optionally, you can update parameter values in the CSV file to match the new device, as required. For example, if the replacement device uses a different interface numbering, as compared with the device being replaced, you can update the parameter that specifies interface numbering.

4. To attach the template to the replacement device, do the following:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

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

   c. In the row for the template that was used for the device being replaced, click **…** and choose **Attach Devices**.
   d. In the **Attach Devices** window, move the replacement device to the **Selected Devices** pane and click **Attach**.
   e. Optionally, you can update parameters in the template before applying it to the device, using one of the following methods:
      - In the row of the replacement device, click **…** and choose **Edit Device Template**. Edit any parameters, as needed.
      - Upload the CSV file that you downloaded and edited to update the parameters for the replacement device. To upload the CSV file, click **Upload** (up arrow button) and navigate to the CSV file.

E. Onboard the new device

Use one of the following methods to onboard the new device.

Note The methods for onboarding a new device to the inventory are relevant to onboarding devices in general. They are not unique to replacing a device.

- Plug and Play (PnP)

  For information, see the Plug and Play Onboarding Workflow section of the Cisco Catalyst SD-WAN Getting Started Guide, and see the Cisco Catalyst SD-WAN: WAN Edge Onboarding guide.

- Bootstrap

  For information, see the Non-PnP Onboarding section of the Cisco Catalyst SD-WAN Getting Started Guide, and see the bootstrap deployment section of the Cisco Catalyst SD-WAN: WAN Edge Onboarding guide.

- Manual deployment

Note To configure the new device, you can use the configuration files that you saved earlier in part A.

Note The manual deployment method requires installing a root certificate authority (CA) for the new device.

For information, see the Cisco Catalyst SD-WAN: WAN Edge Onboarding guide.

For information about installing a root CA, see the Enterprise Certificates section of the Cisco Catalyst SD-WAN Getting Started Guide.

Using Cisco Catalyst SD-WAN Manager on Different Servers

. You can perform the following operations in parallel from one or more Cisco SD-WAN Manager servers:

- From the Cisco SD-WAN Manager menu, select **Maintenance** > **Software Upgrade** to do the following:
  - Upgrade the software image on a device.
  - Activate a software image on a device.
  - Delete a software image from a device.
  - Set a software image to be the default image on a device.
- From the Cisco SD-WAN Manager menu, select **Maintenance** > **Device Reboot** to reboot a device.
- From the Cisco SD-WAN Manager menu, select **Configuration** > **Templates** to manage templates:
  - Attach devices to a device template.
  - Detach devices from a device template.
  - Change the variable values for a device template that has devices attached to it.

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. When you click **Update** > **Configure Devices**, all other template operations—including attach devices, detach devices, and edit device values—are locked on all Cisco SD-WAN Manager servers until the update operation completes. This means that a user on another Cisco SD-WAN Manager server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more Cisco SD-WAN Manager servers, at the same time. However, if any one of these operations is in progress on one Cisco SD-WAN Manager server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Log In to the Cisco Catalyst SD-WAN Manager Web Application Server

The Cisco SD-WAN Manager runs as a web application server through which you log in to a running Cisco SD-WAN Manager.

In an overlay network with a single Cisco SD-WAN Manager, to log in to the server, use HTTPS, and specify the IP address of the server. Enter a URL in the format https://*ip-address*:8443, where 8443 is the port number used by Cisco SD-WAN Manager. On the login page, enter a valid username and password, and then click **Log In**. You have five chances to enter the correct password. After the fifth incorrect attempt, you are locked out of the device, and you must wait for 15 minutes before attempting to log in again.

In an overlay network that has a cluster of Cisco SD-WAN Managers, the cluster allows you to log in to one of the Cisco SD-WAN Managers that is operating in the role of a web application server. Use HTTPS, specifying the IP address of one of the Cisco SD-WAN Managers, in the format https://*ip-address*:8443. The cluster software load-balances login sessions among the individual Cisco SD-WAN Managers that are acting as web application servers. You cannot control which of the individual Cisco SD-WAN Managers you log in to.

With a Cisco SD-WAN Manager cluster, if you enter invalid login credentials, it might take some time for you to see an invalid login error message, and the amount of time increases as the size of the cluster increases. This delay happens because each Cisco SD-WAN Manager attempts sequentially to validate the credentials. If none of the Cisco SD-WAN Manager servers validate you, only then do you see an invalid login error message.

To determine which Cisco SD-WAN Manager you are logged in to, look in the Cisco SD-WAN Manager toolbar, which is located at the top of the screen. To view more information about this particular Cisco SD-WAN Manager server, enter the name of the server in the Search filter of the **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: To determine which Cisco SD-WAN Manager you are logged in to, look in the Cisco SD-WAN Manager toolbar, which is located at the top of the screen. To view more information about this particular Cisco SD-WAN Manager server, enter the name of the server in the Search filter of the **Monitor** > **Network**.