Certificate Management

- Feature history, on page 1
- Manage Certificates in Cisco Catalyst SD-WAN Manager, on page 2
- How Cisco SD-WAN Manager installs a new certificate on an edge device, on page 13
- Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices Using Cisco SD-WAN Manager, on page 14
- Information About Configure CA Certificates Using Cisco SD-WAN Manager, on page 14
- Supported Devices for Uploading CA Certificates, on page 14
- Prerequisites to Configuring CA Certificates, on page 15
- Restrictions for Uploading CA Certificates, on page 15
- Upload CA Certificates, on page 15
- Configure CA Certificates Using Cisco SD-WAN Manager, on page 16
- Monitor CA Certificates and PKI Trustpoints, on page 17
- CRL-Based Quarantine, on page 18
- Manage Root Certificate Authority Certificates in Cisco Catalyst SD-WAN Manager, on page 20
- Enterprise Certificates, on page 21
- Cisco PKI Controller Certificates, on page 30
- Install a web server certificate, on page 36

Feature history

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

Table 1: Feature history

Feature name	Release information	Feature description
Staging for certificate installation on WAN edge devices	Cisco Catalyst SD-WAN Control Components Release 20.18.1 Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	When Cisco SD-WAN Manager installs a new certificate on a WAN edge device, the device first tests the certificate in a staging step before proceeding with installing the certificate. The device verifies that it can successfully establish control connections using the certificate.

Feature name	Release information	Feature description
Web server certificate installation	aaCisco Catalyst SD-WAN Control Components Release 26.1.1	SD-WAN Manager uses an authentication certificate for secure browser connections. This release provides new installation options for web server certificates: • Enterprise certificate support with SCEP and EST protocols • Certificate renewal option • Automatic propagation of a certificate across all SD-WAN Manager instances • Ability for tenants in a multitenant environment to install a certificate of their own

Manage Certificates in Cisco Catalyst SD-WAN Manager

Perform certificate operations in Cisco SD-WAN Manager on the **Configuration** > **Certificates** page.

- Top bar—On the left are the menu icon, for expanding and collapsing the Cisco SD-WAN Manager menu, and the Cisco SD-WAN Manager product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Certificates.
- WAN Edge List tab—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - Send to Controllers—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - Table of WAN edge routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Controllers tab—Install certificates and download the device serial numbers to the Cisco SD-WAN Validator.

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

  - Send to Cisco SD-WAN Validator—Send the controller serial numbers to the Cisco SD-WAN Validator.

- Install Certificate—Install the signed certificates on the controller devices. This button is available only if you select Manual in **Administration** > **Settings** > **Certificate Signing by Symantec**.
- Export Root Certificate—Display a copy of the root certificate for the controller devices that you can download to a file.
- Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Certificate status bar—Located at the bottom of the screen, this bar is available only if you select Server Automated in **Administration** > **Settings** > **Certificate Authorization**. It displays the states of the certificate installation process:
  - Device Added
  - Generate CSR
  - Waiting for Certificate
  - Send to Controllers

  A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.

  From SD-WAN Manager 20.12.1, dates in the exported file use the Unix epoch format.
- Show Table Fields icon—Click the icon to display or hide columns from the device table. By default, all columns are displayed.

Check the WAN Edge Router Certificate Status

In the **WAN Edge List** tab, check the **Validate** column. The status can be one of the following:

- Valid (shown in green)—The router's certificate is valid.
- Staging (shown in yellow)—The router is in the staging state.
- Invalid (shown in red)—The router's certificate is not valid.

Validate a WAN Edge Router

When you add Cisco vEdge devices and WAN routers to the network using the **Configuration** > **Devices** screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox Validate the uploaded WAN Edge List and send to controllers. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the **WAN Edge List** tab, select the router to validate.
2. In the **Validate** column, click **Valid**.

3. Click **OK** to confirm the move to the valid state.
4. Repeat the steps above for each router you wish to validate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco SD-WAN Manager NMS displays the Push WAN Edge List screen showing the status of the push operation.

Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the Cisco SD-WAN Manager instance. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the Cisco SD-WAN Controller and the Cisco SD-WAN Manager instance.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the **Validate** column, click **Staging**.
3. Click **OK** to confirm the move to the staging state.
4. Click **Send to Controllers** in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. Cisco SD-WAN Manager NMS displays the **Push WAN Edge List** screen showing the status of the push operation.
5. To unstage, validate the WAN Edge Router.

Invalidate a WAN Edge Router

1. In the **WAN Edge List** tab, select the router to invalidate.
2. In the **Validate** column, click **Invalid**.
3. Click **OK** to confirm the move to the invalid state.
4. Repeat the steps above for each router you wish to invalidate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco SD-WAN Manager instance displays the **Push WAN Edge List** screen showing the status of the push operation.

Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator

To determine which controllers in the overlay network are valid, the Cisco SD-WAN Validator keeps a list of the controller serial numbers. The Cisco SD-WAN Manager instance learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the Cisco SD-WAN Validator:

1. In the **Controllers** tab, check the certificate status bar at the bottom of the screen. If the **Send to Controllers** check mark is green, all serial numbers have already been sent to the Cisco SD-WAN Validator. If it is grey, you can send one or more serial numbers to the Cisco SD-WAN Validator.

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

2. Click the **Send to Validator** button in the **Controllers** tab. The controller's serial number and the UUIDs of the validated routers are sent to the Cisco SD-WAN Validator. If all serial numbers have been sent, when you click **Send to Validator**, an error message is displayed. To resend a controller's serial number, you must first select the device and then select **Invalid in the Validity** column.

Note In Cisco IOS XE Catalyst SD-WAN Release 17.14.x and earlier, when you click the **Send to Validator** button in the **Controllers** tab, only the controller's serial number is sent once to the Cisco SD-WAN Validator.

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

After the serial numbers have been sent, click the **Tasks** icon in the Cisco SD-WAN Manager toolbar to display a log of the file download and other recent activities.

Install Signed Certificate

If in **Administration** > **Settings** > **Certificate Signing by Symantec**, you selected the **Manual** option for the certificate-generation process, use the **Install Certificate** button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the **Controllers** tab, click **Install Certificate**.

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

2. In the **Install Certificate** window, select a file, or copy and paste the certificate text.
3. Click **Install** to install the certificate on the device. The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps the steps above to install additional certificates.

Export Root Certificate

1. In the **Controllers** tab, click the **Export Root Certificate** button.

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

2. In the **Export Root Certificate** window, click **Download** to export the root certificate to a file.
3. Click **Close**.

View a Certificate Signing Request

1. In the WAN Edge List or **Controllers** tab, select a device.

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

2. Click the **More Actions** icon to the right of the row, and click **View CSR** to view the certificate signing request (CSR).

View a Device Certificate Signing Request

1. In the **WAN Edge List** or **Controllers** tab, select a Cisco IOS XE Catalyst SD-WAN device.

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

2. Click the **More Actions** icon to the right of the row, and click **View Device CSR** to view the certificate signing request (CSR).

   For a Cisco IOS XE Catalyst SD-WAN device where trustpoint has been configured, clicking the **More Actions** icon allows you to view three options:

   - View Device CSR
   - Generate Feature CSR
   - View Feature CSR

Note Cisco SD-WAN Manager will generate alarms only if device certificate is installed through Cisco SD-WAN Manager. If you install certificate manually, Cisco SD-WAN Manager will not generate alarms for certificate expiration.

View the Certificate

1. In the **Controllers** tab, select a device.

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

2. Click the **More Actions** icon to the right of the row and click **View Certificate**.

Generate a Certificate Signing Request

The following procedures describe the process of generating CSRs.

Generate a controller certificate signing request, through SD-WAN Manager 20.16.x

Note From SD-WAN Manager 20.18.1, this procedure has been replaced. Use the Control Components Certificate Management workflow instead.

Procedure

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

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

3. For the desired controller, click **…** and choose **Generate CSR**.

   The **Generate CSR** window is displayed.
4. In the **Generate CSR** window, click **Download** to download the file to your local PC (that is, to the PC you are using to connect to SD-WAN Manager).
5. Repeat the preceding steps to generate a CSR for another controller.

Generate a feature certificate signing request, through SD-WAN Manager 20.16.x

Note From SD-WAN Manager 20.18.1, this procedure has been replaced. Use one of these instead:

- Control Components Certificate Management workflow
- WAN Edges Certificate Management workflow

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired device, click **…** and choose **Generate Feature CSR**.

   The **Generate Feature CSR** window is displayed.
4. In the **Generate Feature CSR** window, click **OK** to continue with the generation of feature CSR. This step authenticates the device trustpoint that has been set and extracts the CSR from the device.
5. Repeat the steps above for each device for which you are generating a CSR.

Generate a WAN edge device certificate signing request, through SD-WAN Manager 20.16.x

Note From SD-WAN Manager 20.18.x, this procedure has been replaced. Use the WAN Edges Certificate Management workflow instead.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired device, click **…** and choose **Renew Device CSR**.

   The **Renew Device CSR** window is displayed.
4. In the **Renew Device CSR** window, click **OK** to continue with the generation of a new CSR.

Note Cisco vManage Release 20.9.1 and later releases: Clicking **Renew Device CSR** resets the RSA private and public keys, and generates a CSR that uses a new key pair. SD-WAN Manager also resets RSA private and public keys before generating a new CSR in Cisco vManage Release 20.6.4 and later Cisco vManage 20.6.x releases.

SD-WAN Manager releases other than the above-mentioned releases: Clicking **Renew Device CSR** generates a CSR using the existing key pair.

Reset the RSA Key Pair

1. In the **Controllers** tab, select a device.

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

2. Click the **More Actions** icon to the right of the row and click **Reset RSA**.

3. Click **OK** to confirm resetting of the device's RSA key and to generate a new CSR with new public or private keys.

Invalidate a Control Component

When invalidating the last remaining Cisco SD-WAN Validator or Cisco SD-WAN Controller in a fabric, Cisco SD-WAN Manager prompts you to set a maintenance window time in which to invalidate the component. Set a time 5 minutes or more from the current time.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** > **Control Components**.
2. In the **Control Components** tab, select an SD-WAN Control Component instance.

   In releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, the tab is called **Controllers**.
3. Adjacent to the SD-WAN Control Component instance, click **...** and choose **Invalidate**.

View Log of Certificate Activities

To view the status of certificate-related activities:

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

View a Signed Certificate

Signed certificates are used to authenticate Cisco SD-WAN devices in the overlay network. To view the contents of a signed certificate using Cisco SD-WAN Manager:

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

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

3. For the desired device, click **...** and choose **View Certificate** to view the installed certificate.

Certificate Revocation

Table 2: Feature History

Feature Name	Release Information	Feature Description
Certificate Revocation	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature revokes enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.

Information About Certificate Revocation

If you are using enterprise certificates with Cisco Catalyst SD-WAN, you can enable Cisco SD-WAN Manager to revoke designated certificates from devices, as needed. For example, you might need to revoke certificates if there has been a security issue at your site.

Note The certificate revocation feature is disabled by default.

Cisco SD-WAN Manager revokes the certificates that are included in a certificate revocation list (CRL) that Cisco SD-WAN Manager obtains from a root certificate authority (CA).

When you enable the Certificate Revocation feature and provide the URL of the CRL to Cisco SD-WAN Manager, Cisco SD-WAN Manager polls the root CA at a configured interval, retrieves the CRL, and pushes the CRL to Cisco IOS XE Catalyst SD-WAN devices, Cisco vEdge devices, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers in the overlay network. Certificates that are included in the CRL are revoked from devices.

When certificates are revoked, they are marked as not valid. Device control connections remain up until the next control connection flap occurs, at which time device control connections are brought down. To bring a device control connection back up, reinstall a certificate on the device and onboard the device.

When Cisco SD-WAN Manager revokes certificates from devices, the devices are not removed from the overlay network, but they are prevented from communicating with other devices in the overlay network. A peer device rejects a connection attempt from a device whose certificate is in the CRL.

Restrictions for Certificate Revocation

- By default, the Certificate Revocation feature is disabled. When you enable the Certificate Revocation feature for the first time, control connections to all the devices in the network flap. We recommend that you enable the feature for the first time during a maintenance window to avoid service disruption.

  When you disable the Certificate Revocation feature, control connections to all the devices in the network flap. We recommend that you disable the feature during a maintenance window to avoid service disruption

- You can use the Certificate Revocation feature only if you are using an enterprise CA to sign certificates for hardware WAN edge certificate authorization, controller certificate authorization, or WAN edge cloud certificate authorization.

- Cisco SD-WAN Manager can connect to a server to retrieve a CRL only through the VPN 0 interface.

Note Starting from Cisco vManage Release 20.11.1, connections through the VPN 512 are supported.

Configure Certificate Revocation

Before You Begin

Make a note of the URL of the root CA CRL.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Administration Settings** window, click **Edit** next to **Certificate Revocation List**.

   The certificate revocation options appear.
3. Click **Enabled**.
4. In the **CRL Server URL** field, enter the URL of the CRL that you created on your secure server.
5. In the **Retrieval Interval** field, enter the interval, in hours, at which Cisco SD-WAN Manager retrieves the CRL from your secure server and revokes the certificates that the CRL designates.

   Enter a value from 1 to 24. The default retrieval interval is 1 hour.
6. Click **Save**.

   Cisco SD-WAN Manager immediately retrieves the CRL and revokes the certificates that the CRL designates. From then on, Cisco SD-WAN Manager retrieves the CRL according to the retrieval interval period that you specified.

Cisco PKI Certificates

Feature Name	Release Information	Description
Support for Cisco PKI Certification	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature allows Cisco SD-WAN Manager to transition from vManage signed certificates to Cisco PKI as the default certificate method for virtual routers to enhance security and reliability.

Cisco PKI Certificates

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

Cisco SD-WAN public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

PKI provides a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or a device) participating in the secured

communicated is enrolled in the PKI in a process where the entity generates an Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has their identity validated by a trusted entity also known as a CA or trustpoint.

Before Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager signed certificates were installed on the controller devices by default. From Cisco Catalyst SD-WAN Manager Release 20.18.1, Virtual routers use a Cisco PKI certificate by default. After you reset a WAN edge device, you have to install the certificates manually on the device. If you perform an upgrade, your certificate is retained.

Note When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1 or later, the Cisco SD-WAN Controllers continues to support Cisco SD-WAN Manager signed certificate if it is already enabled. However, when the certificates are renewed, the Cisco SD-WAN Controllers have a PKI certificate by default.

Renew a Certificate

Before You Begin

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Certificate settings**. Click any one of the following options and choose enterprise mode to enable the CRL (certificate revocation list).
  - In the **Certificate Signing by** field, choose **Cisco (Recommended)** or **Manual** or **Enterprise Certificate** .
  - When you choose **Cisco (Recommended)**, click **Sync Root Certificate** to sync root certificate to all the connected devices.
  - In the **Validity Period** field, choose the duration.
  - Click **Save**.

Note By default, the **Cisco (Recommended)** option is disabled.

To renew Certificates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired controller, click **…** and choose **Renew CSR**.

   The **Renew CSR** window is displayed.

The certificates are renewed in the following order:

1. Cisco SD-WAN Manager
2. Cisco SD-WAN Validator
3. Cisco SD-WAN Controller

4. Cisco IOS XE Catalyst SD-WAN device

Note When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1 or later, the Cisco SD-WAN Controllers continues to support vManage signed certificate if it is already enabled. However, when the certificates are the renewed, the Cisco SD-WAN Controllers have PKI certificate by default.

How Cisco SD-WAN Manager installs a new certificate on an edge device

In a Cisco Catalyst SD-WAN environment, edge devices use certificates for authorization when establishing control connections with SD-WAN Control Components. From SD-WAN Manager 20.18.1, when SD-WAN Manager installs a new certificate on a device, the device first tests the certificate in a staging step before proceeding with installing the certificate. During the staging step, the device verifies that it can successfully establish a control connection to the SD-WAN Validator, using the certificate. If the SD-WAN Validator cannot validate the certificate, it rejects the connection.

Workflow

1. SD-WAN Manager stages a certificate on a WAN edge device.
2. The device attempts to connect to the SD-WAN Validator, using the staged certificate for authorization. Staging and testing can take a minute or more.
   - If the certificate is valid and if the SD-WAN Validator recognizes the certificate, it accepts the control connection.
   - If the certificate is invalid or if the SD-WAN Validator does not recognize the certificate, it rejects the control connection.
3. The edge device reports the staging result back to SD-WAN Manager: success or failure.
   - In case of success, SD-WAN Manager completes the installation of the certificate on the device.
   - In case of failure, SD-WAN Manager does not proceed to install the certificate, and adds a log entry indicating the failure.

Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices Using Cisco SD-WAN Manager

Table 3: Feature History

Feature Name	Release Information	Description
Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Using Cisco SD-WAN Manager, conveniently upload and push generic third-party CA certificates to Cisco IOS XE Catalyst SD-WAN devices with a Trustpoint name. The provisioning is executed via configuration groups parcel, with the status readily viewable in monitoring.

Information About Configure CA Certificates Using Cisco SD-WAN Manager

The Cisco SD-WAN Manager currently permits the upload of third party certificates to devices during their integration with the Cisco Catalyst SD-WAN fabric, yet this function is only available during the control connection establishment and initial device setup.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the feature enables certificate upload using the UI. The Cisco SD-WAN Manager supports CA certificate uploads even after device setup.

The CA certificates authenticate the server identities and prevent unauthorized access. The Cisco IOS XE Catalyst SD-WAN devices use CA certificates to establish and manage secure connections with different servers in a network. When you upload a CA certificate to Cisco SD-WAN Manager, the Cisco IOS XE Catalyst SD-WAN device uses this certificate information from the configuration group parcels in verifying and authenticating the connections it establishes with servers across a network, thus improving the overall security and integrity of your network traffic.

Note The CA certificates isn't suited for SSL-based access with router trusted roots.

Supported Devices for Uploading CA Certificates

Cisco IOS XE Catalyst SD-WAN devices

Prerequisites to Configuring CA Certificates

- Your Cisco SD-WAN Manager must run Cisco Catalyst SD-WAN Manager Release 20.13.1 and later releases to upload CA certificates.
- Your Cisco IOS XE Catalyst SD-WAN device must run Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and later releases to upload CA certificates.

Restrictions for Uploading CA Certificates

- Supports only PEM encoded certificate files.
- Maximum certificate file size: 10 MB.
- If you are using Cisco Catalyst SD-WAN Multitenancy, you need to be a tenant to upload and manage CA certificates. For more information see, Tenant Role.

Note When you login into Cisco SD-WAN Manager as a provider, you can't upload and manage CA certificates.

Upload CA Certificates

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click the **CA Cert** tab.
3. Click **Add CA Certificate**.
4. In the **Add CA Certificate** pane, enter **Certificate Name**.
5. **Choose a file** or drag and drop to upload a CA certificate.
6. Click the **Paste** tab and paste the certificate details.
7. Click **Save**.

   On the **Certificate Authority** page, find the CA certificate listed in the **Device Group** table.

Note Spot the **Expiration Date** in the **Device Group** table for your CA certificate and perform more **Actions** by clicking the **...** icon.

Delete CA Certificates

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

2. Click the **CA Cert** tab.
3. In the **Device Group** table, select the CA certificate to delete.
4. Click **Delete**.

Note Alternate method to delete a CA certificate: click the **...** icon in the **Actions** column and click **Delete**.

Configure CA Certificates Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Configuration Groups**.

   For more information on creating a configuration group, see Configuration Group Workflows.
2. Add a feature to the configuration group.

   For more information on adding a feature, see Feature Management.
3. Under **System Profile**, click **Add Feature**.
4. In the **Add Feature** pane, choose **CA Certificate**.
5. Configure the **CA Certificates** section.

   Table 4: CA Certificates

Field	Description
Type	Choose **CA Certificate** from the drop-down list.
Name	Enter a name for the certificate.
Description	(Optional) Provide a description for the certificate.
Add CA Certificate	Click **Add CA Certificate** to add additional CA certificates.
TrustPoint Name	Enter a TrustPoint Name.
Certificate Name	Choose a CA certificate to add from the drop-down list.

6. Click **Save**.
7. Deploy the devices associated to the configuration group. For more information, see Deploy Devices.

Note When you modify a certificate from the **Device Group** table, the changes won't be mirrored on the device. This is due to the certificate's association with a TrustPoint. To update the certificate, it's necessary to remove the existing TrustPoint that contains the certificate information. Subsequently, create a new TrustPoint and add the certificate to it. Finally, deploy the changes to the device for the certificates to take effect.

Deleting certificates from the **Certificates** tab doesn't automatically delete the associated TrustPoint. To delete the TrustPoint, you must manually delete and then save the changes to the TrustPoint.

Revoke the CA Certificates

Use the following instructions to revoke a CA certificate:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **...** adjacent to the configuration group name and choose **Edit**.
3. Click the desired system profile.
4. Click **...** adjacent to the CA certificate feature and choose **Delete Feature**.
5. Deploy the changes to the device.

Renew the CA Certificates

Use the following instructions to renew a CA certificate:

1. Upload the CA certificate that you'd like to renew to the Cisco SD-WAN Manager.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
3. Click **...** adjacent to the configuration group name and choose **Edit**.
4. Click the desired system profile.
5. Click **...** adjacent to the CA certificate feature and choose **Delete Feature**.
6. Using **Configuration Groups**, add a feature to the configuration group and follow the instructions from step 3 to step 7 in the **Configure CA Certificate topic**.

Monitor CA Certificates and PKI Trustpoints

Track CA Certificate

Track a CA certificate using the **Issuer Name**, **Certificate Serial No.**, and **Expiration Date** listed in the Cisco SD-WAN Manager.

1. In the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Click the **CA Cert** tab.
3. The CA certificate added to Cisco SD-WAN Manager appears in the **Device Group** table.

Monitor CA Certificate Installation

Once the CA certificate installation is complete, the Cisco IOS XE Catalyst SD-WAN device sends the event logs to Cisco Catalyst SD-WAN Manager.

From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.

The CA certificate installation is listed as an event and appears in the **Events** table.

Monitor PKI Trustpoints

Monitor PKI Trustpoints using the real time command **`PKI Trustpoint`**. For more information, see View PKI Trustpoint information.

CRL-Based Quarantine

Table 5: Feature History

Feature Name	Release Information	Feature Description
CRL-Based Quarantine	Cisco vManage Release 20.11.1	With this feature you can quarantine SD-WAN edge devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a certificate authority.

Information About CRL-Based Quarantine

When you use enterprise certificates with Cisco Catalyst SD-WAN, you can use Cisco SD-WAN Manager to quarantine SD-WAN edge devices that are compromised, and their certificates have been revoked.

Note The certificate revocation list (CRL)-based quarantine feature is disabled by default.

- Cisco SD-WAN Manager revokes the certificates that are included in a certificate revocation list (CRL). Cisco SD-WAN Manager obtains this list from a certificate authority (CA).
- At defined intervals, Cisco SD-WAN Manager polls the CRL server for the latest CRL. On receiving the list, Cisco SD-WAN Manager analyzes it to determine which SD-WAN edge device is to be quarantined.
- Cisco SD-WAN Manager checks if the serial numbers of certificates for each valid SD-WAN edge device in the network match the serial numbers of certificates within the CRL. On finding a match, the certificates on the SD-WAN edge devices are not removed to enable the SD-WAN edge devices to retain a control connection to Cisco SD-WAN Manager.

The quarantine process for SD-WAN edge devices is as follows:

- For each SD-WAN edge device that is quarantined:

- Cisco SD-WAN Manager moves the SD-WAN edge device to the staging mode. The staging mode shuts down data traffic while maintaining a control connection to Cisco SD-WAN Manager.
- Cisco SD-WAN Manager generates notifications for the SD-WAN edge device being quarantined.

For each Cisco SD-WAN Controller that is quarantined, Cisco SD-WAN Manager generates notifications for the controller.

Note The CRL server connects to Cisco SD-WAN Manager through VPN 0 or VPN 512.

Restrictions for CRL-Based Quarantine

- You can use the CRL-based quarantine feature only if you have an enterprise CA (certificate authority) to sign certificates for hardware WAN edge certificate authorization, controller certificate authorization, or WAN edge cloud certificate authorization.
- Disable the CRL to switch from certificate revocation to quarantine or quarantine to certificate revocation. You cannot enable the certificate revocation and CRL-based quarantine option at the same time.

Configure CRL-Based Quarantine

Before You Begin

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**. Click any one of the following options and choose enterprise mode to enable the CRL (certificate revocation list).
  - In the **Controller Certificate Authorization** field, choose **Enterprise Root Certificate** or
  - In the **Hardware WAN Edge Certificate Authorization** field, choose **Enterprise Certificate (signed by Enterprise CA)** or
  - In the **WAN Edge Cloud Certificate Authorization** field, choose **Manual (Enterprise CA - recommended)**.
- Make a note of the URL of the CA CRL.

Note By default, the CRL-based quarantine feature is disabled.

To configure CRL-based quarantine:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Administration Settings** page, click **Edit** next to **Certificate Revocation List**.

   The Certificate Revocation and CRL-Based Quarantine options appear.
3. Click **CRL-Based Quarantine**.

4. In the **CRL Server URL** field, enter the URL of the CRL that you created on your secure server.
5. In the **Retrieval Interval** field, enter the interval in hours. Cisco SD-WAN Manager uses the certificate revocation list (CRL) to quarantine SD-WAN edge devices.

   Enter a value from 1 to 24. The default retrieval interval is 24 hours.
6. Click **VPN 0** or **VPN 512**. Cisco SD-WAN Manager connects to a server to retrieve the CRL through the VPN 0 or VPN 512 interface.
7. Click **Save**.

   Cisco SD-WAN Manager at intervals, polls the CRL server for the latest CRL. This list is analyzed to determine which SD-WAN edge devices are to be quarantined.

Note If the CRL is disabled in earlier releases, the CRL remains disabled after upgrading to the Cisco vManage Release 20.11.1. If the CRL was enabled in a release prior to Cisco vManage Release 20.11.1, then after upgrading to Cisco vManage Release 20.11.1, the certificate revocation option is enabled with VPN0 as the default.

Manage Root Certificate Authority Certificates in Cisco Catalyst SD-WAN Manager

Feature Name	Release Information	Description
Support for Managing Root CA Certificates in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature enables you to add and manage root certificate authority (CA) certificates.

Add a Root Certificate Authority Certificate

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. In the **Root Certificate** field, paste in certificate text, or click **Select a File** to load a certificate from a file.
4. Click **Add**. The new certificate appears in the certificate table. The **Recent Status** column indicates that the certificate has not yet been installed.
5. Click **Next** and review the details of any certificates that have not been installed.
6. Click **Save** to install the certificate(s). The new certificate appears in the certificate table.

View a Root Certificate Authority Certificate

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. (optional) In the search field, enter text to filter the certificate view. You can filter by certificate text or attribute values, such as serial number.
3. In the table of certificates, click **More Actions** (**…**) and choose **View**. A pop-up window appears, displaying the certificate and its details.

Delete a root certificate

Before you begin

Note When you make changes to the root certificate chain, SD-WAN Manager automatically propagates the changes to SD-WAN Validator and SD-WAN Controller instances.

Use this procedure to delete a root Certificate Authority (CA) certificate.

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. Select one or more root certificates in the table and click the **trash** icon in the **Action** column. The table shows the certificate as marked for deletion.
4. Click **Next** and review the details of any certificates that are marked for deletion.
5. Click **Save** to delete the certificate(s).

Enterprise Certificates

Feature Name	Release Information	Description
RSA Key Length Increase in Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Control Components Release 20.15.2 Cisco Catalyst SD-WAN Control Components Release 20.16.1	Introduces 4096-bit RSA key support for certificate signing requests (CSR) for enterprise certificates.

In Cisco IOS XE SD-WAN Release 16.11.1 and Cisco SD-WAN Release 19.1, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization used previously. For purposes of certificate management, the term *controller* is used to collectively refer to Cisco SD-WAN Manager, the Cisco Catalyst SD-WAN Controller, and the Cisco Catalyst SD-WAN Validator.

RSA Key Length

When using enterprise certificates for Cisco SD-WAN Controllers, ensure that you use root certificates with an RSA key that is at least 2048 bits.

From Cisco Catalyst SD-WAN Control Components Release 20.16.1 and Cisco Catalyst SD-WAN Control Components Release 20.15.2, Cisco SD-WAN Control Components support RSA key sizes ranging from 2048 to 4096 bits.

Downgrade Restriction

If you are using enterprise certificates that use 4096-bit RSA keys, before downgrading Cisco SD-WAN Control Components to a release earlier than Cisco Catalyst SD-WAN Control Components Release 20.16.1Cisco Catalyst SD-WAN Control Components Release 20.15.2, change the enterprise certificates to use 2048-bit RSA keys.

Note For more information about enterprise certificates, see the Cisco Catalyst SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide.

Use the Certificates page to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco Catalyst SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from Cisco SD-WAN Manager that you generate these certificates and install them on the controller devices—Cisco SD-WAN Manager, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers.
- The WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco Catalyst SD-WAN, mark each router as valid or invalid, and then from Cisco SD-WAN Manager, send the file to the controller devices in the network.

Install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

Configure Enterprise Certificates for Cisco SD-WAN Controllers

Feature Name	Release Information	Description
Support for Secondary Organizational Unit	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco SD-WAN Release 20.1.1	This optional feature allows you to configure a secondary organizational unit when configuring the certificates. If specified, this setting is applied to all controllers and edge devices.
Support for Subject Alternative Name (SAN)	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature enables you to configure subject alternative name (SAN) DNS Names or uniform resource identifiers (URIs). It enables multiple host names and URIs to use the same SSL certificate.

Feature Name	Release Information	Description
Support for Specifying Any Organization for WAN Edge Cloud Device Enterprise Certificates	Cisco Catalyst SD-WAN Control Components Release 20.11.1	When configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization in the **Organization** field. You are not limited to names such as **Viptela LLC**, **vIPtela Inc**, or **Cisco Systems**. This enables you to use your organization's certificate authority name or a third-party certificate authority name.
Support for Certificates Without the Organizational Unit Field	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Control Components Release 20.12.1	Enterprise certificates that you install on devices do not require the Organizational Unit (OU) field to be defined. Earlier, this field was used as part of the authentication of a device.

Information About Enterprise Certificates

Enterprise certificates allow organizations to use their own private certificate signing authority rather than having to rely on public certificate signing authorities. You can also apply custom certificate properties using the **Set CSR Properties** field.

Note In the 16.11/19.1 release, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization that were used previously. An independent organization handles the signing of enterprise certificates.

Use the **Configuration** > **Certificates** page to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco Catalyst SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from Cisco SD-WAN Manager that you generate these certificates and install them on the controller devices—Cisco SD-WAN Manager instances, Cisco SD-WAN Validators, and Cisco SD-WAN Controller.
- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco Plug and Play (PnP), mark each router as valid or invalid, and then from Cisco SD-WAN Manager, send the file to the controller devices in the network.

You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

Note For purposes of certificate management, the term controller refers collectively to Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.

Once you reset a WAN edge device, you have to install the enterprise root certificate manually on the device. If you perform an upgrade, your certificate is retained.

Note Cisco SD-WAN Manager supports only Base 64 encoded certificates. Other formats, such as DER, encoded are not supported.

For example, the PEM extension is used for different types of X.509v3 files that contain ASCII (Base64) armored data prefixed with a **--BEGIN ...** line.

Dependency on OU Fields in Enterprise Certificates

From Cisco Catalyst SD-WAN Control Components Release 20.12.1, when onboarding a device, Cisco Catalyst SD-WAN does not require that the associated enterprise certificate have any OU fields defined. However, if at least one OU field is defined, then Cisco Catalyst SD-WAN requires that one of the OU fields match the organization name of the fabric.

From Cisco Catalyst SD-WAN Control Components Release 20.12.2, when onboarding a device, if the associated enterprise certificate has one or more OU fields defined, the OU fields need not match the organization name of the fabric.

Devices that Support Enterprise Certificates

Device	Enterprise Certificate Support
Cisco SD-WAN Manager	Yes
Cisco SD-WAN Validator	Yes
Cisco SD-WAN Controller	Yes
Edge routers	All hardware WAN edge routers vEdge/IOS-XE-SD-WAN except ASR1002-X, ISRv, CSR1000v

Web server certificate for SD-WAN Manager

Cisco SD-WAN Manager uses an authentication certificate for secure browser connections. There are three methods for installing a certificate:

- Assign SD-WAN Manager itself to sign the certificate.
- Install an enterprise certificate using an automatic method, which makes use of the SCEP or EST protocols.
- Install an enterprise certificate using a manual method, in which you generate a CSR, get it signed, and upload the signed certificate.

Certificate renewal

You can renew an existing certificate before it reaches its expiration date by clicking a Renew option.

Multitenancy

Individual tenants in a multitenant Cisco Catalyst SD-WAN environment (a) can use the certificate installed by the provider, or (b) can install a certificate of their own.

Propagation across all SD-WAN Manager instances

When you install a web server certificate on one SD-WAN Manager node, SD-WAN Manager installs the certificate across all other SD-WAN Manager instances, within a cluster and across clusters. The time required to propagate a certificate across all instances depends on numerous factors.

Configure Enterprise Certificates

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Hardware WAN Edge Certificate Authorization**.
2. Click **Enterprise Certificate** (signed by Enterprise CA).

   On Box Certificate (TPM/SUDI Certificate) is the default option.
3. If you want to specify custom certificate properties, click **Set CSR Properties** and configure the following properties.

Property	Description
Domain Name	Network domain name. Do not exceed 17 characters.
Organizational Unit	This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. **Note** For devices using Cisco IOS XE Catalyst SD-WAN Release 17.9.3a or later releases of Cisco IOS XE Release 17.9.x, or Cisco IOS XE Catalyst SD-WAN Release 17.12.1a or later, the certificates that you install on the devices do not require the Organizational Unit field to be defined. However, if a signed certificate includes the Organizational Unit field, the field must match the organization name configured on the device. This addresses the policy of the Certification Authority Browser Forum (CA/Browser Forum), as of September 2022, to stop including an organizational unit in signed certificates. Despite the change in policy of the CA/Browser Forum, some certificate authorities might still include an organizational unit in the signed certificate.

Property	Description
Secondary Organization Unit	This optional field is available from Cisco IOS XE Release 17.2 or Cisco SD-WAN Release 20.1.x. If this optional field is specified, it will be applied to all controllers and edge devices. **Note** If a signed certificate includes the Organizational Unit field or the Secondary Organizational Unit field, one of these fields must match the organization name configured on the device. This addresses the policy of the Certification Authority Browser Forum (CA/Browser Forum), as of September 2022, to stop including an organizational unit in signed certificates. Despite the change in policy of the CA/Browser Forum, some certificate authorities might still include an organizational unit in the signed certificate.
Organization	Organization name.
City	City name.
State	State name.
Email	Email address.
2-Letter Country Code	Country code.
Subject Alternative Name (SAN) DNS Names	Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com
Subject Alternative Name (SAN) URIs	Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

4. Choose **Select a file** to upload a root certificate authority file.

   The uploaded root certificate authority displays in the text box.

5. Click **Save**.

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

7. Select the **Upload WAN Edge List** tab.

8. Browse to the location of the Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices list and click **Upload**.

9. On the **Configuration** > **Certificates** page, click **...** and choose an action:

   - **View Enterprise CSR** (certificate signing request): Copy the CSR and sign it using the enterprise root certificate, and upload the signed certificate on Cisco SD-WAN Manager using the Install Certificate operation. Cisco SD-WAN Manager automatically discovers on which hardware edge the certificate needs to be installed on.
   - **View Enterprise Certificate**: After the certificate is installed, you can see the installed certificate and download it.

- **Renew Enterprise CSR**: If you need to install a new certificate on the hardware device, you can use the Renew Enterprise CSR option. The Renew Enterprise CSR option generates the CSR. You can then view the certificate (View Enterprise CSR option) and install the certificate (Install Certificate option). This step flaps the control connections as a new serial number. You can see the new serial number and expiry data on the Configuration > Certificates page.

Note The certificates that you install on devices in the Cisco Catalyst SD-WAN overlay do not require the Organizational Unit field to be defined. However, if a signed certificate includes the Organizational Unit field, the field must match the organization name configured on the device.

- **Revoke Enterprise Certificate**: This option removes the enterprise certificate from the device and moves it back to prestaging. The device has only Cisco SD-WAN Validator and Cisco SD-WAN Manager controls up.

For a Cisco IOS XE Catalyst SD-WAN device, click **...** and choose an action:

- **View Feature CSR**:
  - Copy the CSR available from the Cisco IOS XE Catalyst SD-WAN device.
  - Sign the certificate using the enterprise root certificate from a certifying authority.
  - Upload the signed certificate on Cisco SD-WAN Manager using the **Install Feature Certificate** operation.

    Cisco SD-WAN Manager automatically discovers on which hardware edge the certificate needs to be installed. After you install feature certificate, the option **View Feature Certificate** is available.

- **View Feature Certificate**: After you install the feature certificate, you can view the feature certificate and download it.
- **Revoke Feature Certificate**: This option removes the feature certificate or trustpoint information from the Cisco IOS XE Catalyst SD-WAN device. After revoking a certificate, all actions against devices are not available. To view all actions for a device, ensure that you configure logging information of the device to a Transport Layer Security (TLS) profile with authentication type as server, and then configure back to mutual. Alternatively, to view the actions, reset Cisco IOS XE Catalyst SD-WAN device to factory default configuration.

  To reset a device to factory default:
  - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
  - Create a device template with the factory-default template.

    The factory-default template is, Factory_Default_*feature-name*_Template. See Create a Device Template from Feature Templates for information about creating a device template with feature template.

10. Click **Install Certificate** or **Install Feature Certificate** to upload the signed certificate.

    The certificate must be a signed certificate. Initially, the state is CSR Generated.

The state changes to Certificate Installed when successfully installed.

11. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**. You can see enterprise certificate columns, including the device type, chassis-id, enterprise serial number, and enterprise certificate date.

Invalidate a Device Certificate

Before deleting a WAN edge device, invalidate the device.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. In the row showing the device, click **Invalid** to invalidate the device.

Authorize a Controller Certificate for an Enterprise Root Certificate

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In the **Controller Certificate Authorization** area, click **Edit**.
3. Click **Enterprise Root Certificate**. If a warning appears, click **Proceed** to continue.
4. Optionally, click **Set CSR Properties** to configure certificate signing request (CSR) details manually.

Note In a multi-tenant scenario, if you configure CSR properties manually and if you are using Cisco Catalyst SD-WAN Control Components Release 20.11.1 or later, then ensure that devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.11.1a or later. In a single-tenant scenario, this is not required.

In a multi-tenant scenario, if you configure CSR properties manually, then when you are ready to generate a CSR for a tenant device, enter the tenant's organization name in the **Secondary Organizational Unit** field described below. In a multi-tenant scenario, if you are generating a CSR for a service provider device, this is not required.

The following properties appear:

- **Domain Name**: Network domain name. Maximum 17 characters.
- **Organizational Unit**

Note **Organizational Unit** is a noneditable field. This field is auto-filled with the organization name that you have configured for Cisco SD-WAN Manager in **Administration** > **Settings** > **Organization Name**.

- **Secondary Organizational Unit**: This optional field is only available in Cisco IOS XE Release 17.2 or Cisco SD-WAN Release 20.1.x and onwards. Note that if this optional field is specified, it will be applied to all controllers and edge devices.
- **Organization**: Beginning with Cisco vManage Release 20.11.1, when configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization

in this field. You are not limited to names such as **Viptela LLC**, **vIPtela Inc**, or **Cisco Systems**. This enables you to use your organization's certificate authority name or a third-party certificate authority name. The maximum length is 64 characters, and can include spaces and special characters. Cisco SD-WAN Manager validates the name when you enter it.

- **City**
- **State**
- **Email**
- **2-Letter Country Code**
- **Subject Alternative Name (SAN) DNS Names**: (optional) You can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com
- **Subject Alternative Name (SAN) URIs**: (optional) You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

5. Paste an SSL certificate into the **Certificate** field or click **Select a file** and navigate to an SSL certificate file.
6. (Optional) In the **Subject Alternative Name (SAN) DNS Names** field, you can enter multiple host names to use the same SSL certificate.

   Example: cisco.com and cisco2.com
7. (Optional) In the **Subject Alternative Name (SAN) URIs** field, you can enter multiple URIs to use the same SSL certificate.

   Example: cisco.com and support.cisco.com

   This is helpful for an organization that uses a single certificate for a host name, without using different subdomains for different parts of the organization.

Generate a Bootstrap Configuration

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

Note If you need to generate a bootstrap configuration, use the **Configuration** > **Devices** page, click **…**, and choose **Generate Bootstrap Configuration**.

Note Beginning with Cisco vManage Release 20.7.1, there is an option available when generating a bootstrap configuration file for a Cisco vEdge device, enabling you generate two different forms of the bootstrap configuration file.

- If you are generating a bootstrap configuration file for a Cisco vEdge device that is using Cisco Catalyst SD-WAN Release 20.4.x or earlier, then check the **The version of this device is 20.4.x or earlier** check box.
- If you are generating a bootstrap configuration for a Cisco vEdge device that is using Cisco SD-WAN Release 20.5.1 or later, then do not use the check box.

Cisco PKI Controller Certificates

From software release 19.x and onwards, there is an option to use Cisco as the certificate authority (CA) instead of Symantec/Digicert for Cisco Catalyst SD-WAN controller certificates.

This section describes deployment types, scenarios to administer, install, and troubleshoot controller certificates using Cisco public key infrastructure (PKI). Cisco PKI provides certificate management to support security protocols such IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

The major difference between Symantec/Digicert and Cisco PKI certificates is that Cisco PKI certificates are linked to a Smart Account (SA) and Virtual Account (VA) in Plug and Play (PnP) and do not require manual approval using a portal like Digicert. Each VA has a limit of 100 certificates, meaning that each overlay has a limit of 100 certificates, and after the certificate signing request (CSR) is generated, the approval and installation happens automatically if the Cisco SD-WAN Manager settings are set correctly.

Devices are added and certificates are installed automatically from the Cisco PKI servers. No intervention is required to approve the certificate.

Supported Devices for Cisco PKI Certificates

The following are the supported devices for using Cisco PKI certificates.

Device	Support
Cisco SD-WAN Manager	Yes
Cisco Catalyst SD-WAN Validator	Yes
Cisco Catalyst SD-WAN Controller	Yes
Cisco vEdge devices	Yes
Cisco IOS XE Catalyst SD-WAN devices	Yes

Use Cases for Cisco PKI Controller Certificates

- Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above, on page 31

- Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal, on page 33
- Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers, on page 35

Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above

Prerequisites

Cisco SD-WAN Manager and the controllers should all be running the same software version.

On the **Configuration** > **Devices** > **Controllers** page, ensure that the OOB IP address and credentials are updated for all the controllers.

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

You can verify the software version for the new or expired overlays without having control connections using SSH.

1. SSH to each of the controllers and the version should show during the SSH process.
2. You do not need to actually have the credentials work, therefore you can run this on a controller where the credentials do not work.

   Repeat this process for all the controllers in the overlay to make sure.
3. Customer Smart Account credentials need to be ready using either of the following methods:
   a. Email and request the customer contact from PnP trigger notifications to individually email you and provide the Smart Account credentials.

      or

   b. Email and request the customer contact to log on to Cisco SD-WAN Manager and add them. Also ensure that you ask the customer for their IPs to be added to the allowed list..

      Ensure that if asking the customer to provide their customer contact to log on, this step is done after asking the customer for their IPs to be added to the allowed list, so that they can reach the Cisco SD-WAN Manager GUI, be be able to log in, and input their Smart Account credentials.

      To find your Smart Account credentials, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials** .

      Enter the user name and password and click **Save**.

Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Controller Certificate Authorization** and click **Edit**.
3. Click **Cisco (Recommended)**.

Note Cisco SD-WAN Manager displays an error if the Smart Account credentials are not added. Check the prerequisites.

4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press Save.

Note Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the Cisco SD-WAN Manager GUI.

   From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers**. Click **…** and choose **Generate CSR**.

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

   The operation status shows the CSR sent for signing, the certificate signed and installed automatically without needing human intervention.

7. The certificates are installed automatically. If successful, the **Configuration** > **Certificates** > **Controllers** page shows the following:

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

   - Expiration date for the certificates for each controller
   - Operation Status column:
     - Cisco SD-WAN Validator: "Installed"
     - Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller: "Cisco SD-WAN Validator Updated"
   - Certificate Serial column: Certificate serial number

8. Ensure that the control connections have come up to the controllers on the Cisco SD-WAN Manager dashboard.

Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal

Prerequisites

Cisco SD-WAN Manager, controllers, and vEdges should all have their control connections up.

Ensure OOB IP address and credentials are updated in **Configuration** > **Devices** > **Controllers**.

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

For each controller, click **…** and verify the updates.

Migrate an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates

1. In Cisco SD-WAN Manager, verify that the control connections to controllers and Cisco vEdge devices are up.

   If the control connections are not up, migrating from Digicert to Cisco PKI cannot proceed.

   If the control connections are only partially up, that is some Cisco vEdge devices are control down, then those Cisco vEdge devices will not be able to automatically reconnect to the controllers if their control comes up after the certificates have been moved to Cisco PKI.

   If it is a case of expired certificates and control connections are down, then certificates need to be renewed on Digicert first and control connections need to be brought up before migrating them to the Cisco PKI controller certificates.

2. Verify that the software version of the controllers is 19.x or later.

   How to Verify the Software Version for the Active Existing Overlays (with Valid Control Connections to Controllers) Using Cisco SD-WAN Manager

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

   b. Click **Manager** and check the **Current Version** column. Verify that it is 19.x or later.

      If the control connections are up and Cisco SD-WAN Manager and controller versions are not 19.x or later, then upgrade them first (Cisco vEdge devices need not be upgraded) before migration to Cisco PKI can be done.

Note It is mandatory that controllers upgraded to 19.x should immediately have their certificates renewed with Cisco PKI as part of the upgrade; they cannot be allowed to run with the existing Symantec certificates even if those certificates are going to remain valid.

   c. After verifying the prerequisites, check that the Cisco PKI root-CA has been propagated to all the controllers and the Cisco vEdge devices. This requires SSH access to the controllers.

      1. SSH into the Cisco SD-WAN Manager and controllers and run the following command: **show certificate root-ca-cert | include Cisco**.

If the output is blank or does not show the result, escalate to the cloud infrastructure team.

d. Customer Smart Account credentials need to be ready by either of the following methods:

1. Email and request the customer contact from a PnP trigger notification to individually email you and provide the Smart Account credentials.

   or

2. Email and request your customer contact to log on to the Cisco SD-WAN Manager themselves and add them. Also ensure that you ask for the customer IPs to be added to the allowed list.

   Ensure that if asking the customer to provide, this step is done after asking the customer for their IPs to be added to the allowed list, so that they can reach the Cisco SD-WAN Manager GUI, be able to log on, and input the Smart Account Credentials.

   To view the Smart Account credentials, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and see the **Smart Account Credentials** section.

3. Enter the username and password and click **Save**.

   Once all the prerequisites have been satisfied, follow the **Runbook to Request and Install Cisco PKI Certificates** procedure to request CSRs and get the Cisco certificates installed. Verify that all the control connections to the controllers and the Cisco vEdge devices have come back up. If not, then escalate to the cloud infrastructure team.

Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**, and in the **Controller Certificate Authorization** section, click **Edit**.
3. Click **Cisco (Recommended)**.

Note Cisco SD-WAN Manager displays an error if the Smart Account credentials are not added. Check the prerequisites.

4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press Save.

Note Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the Cisco SD-WAN Manager GUI.

   From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers** . Click **…** and choose **Generate CSR**.

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

The operation status shows the CSR sent for signing, the certificate signed and installed automatically without requiring intervention.

7. The certificates are installed automatically. If successful, the **Configuration** > **Certificates** > **Controllers** page shows the following:

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

- Expiration date for the certificates for each controller
- Operation Status column:
  - Cisco SD-WAN Validator: "Installed"
  - Cisco SD-WAN Manager and Cisco SD-WAN Controller: "Cisco SD-WAN Validator Updated"
- Certificate Serial column: Certificate serial number

8. Ensure that the control connections have come up to the controllers on the Cisco SD-WAN Manager dashboard.
9. Set the Certificate Retrieve Interval to 1 minute.
10. Click **Sync Root Certificate** to migrate the Cisco vEdge devices or Cisco IOS XE Catalyst SD-WAN devices in Cisco SD-WAN Manager to Cisco pki. This support available from 19.2.1 version or later.
11. Click **Save**.

Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers

The following steps require access to PnP and to the SA/VA in question. Customers have access to their own SA/VA.

Prerequisites

The prerequisites are the same in the above cases, except that you use the manual method for installing the certificates.

Runbook

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**. In the **Controller Certificate Authorization** section, verify that it is set to Manual.
2. Generate the CSRs for the controllers.

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

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

Click **…** and choose **Generate CSR**.

Download each CSR to a file with a filename `.csr` and keep it ready to submit to the PnP portal for getting the signed certificates.

3. Log on to the PnP portal to the required SA/VA and select the Certificates tab.
4. Click **Generate Certificate** and follow the steps to give a name for the certificate file, paste the CSR, and download the signed certificate.

   The finished certificate is ready for download. Repeat this process for each CSR and download all the required certificates.
5. To install the downloaded certificates, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates** and click **Controllers**.

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

Click **Install Certificate**.

After installation, verify that the control connections are up.

Debugging and Log Information

1. Check the Cisco Catalyst SD-WAN Validator profile under the VA in PnP to verify that the correct organization name exists.
2. Check the output at `/var/log/nms/vmanage-server.log` on Cisco SD-WAN Manager for logs of the entire certificate process.
3. Verify that Cisco SD-WAN Manager has internet connectivity to reach the Cisco PKI servers.

Install a web server certificate

Before you begin

To use the automatic option in this procedure, first configure either EST (Enrollment over Secure Transport) or SCEP (Simple Certificate Enrollment Protocol), which are certificate enrollment protocols, in **Administration** > **Settings** > **Certificate settings** > **Enterprise certificate settings**.

Procedure

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

Step 2 If you have a certificate installed and wish to renew it before it expires, select **Renew** adjacent to the installed certificate shown in the **Installed certificate details** area.

Step 3 To install a new certificate, select an installation option.

Option	Description
SD-WAN Manager signed	Generate a certificate signing request (CSR), to be signed by a root certificate authority (CA) installed on SD-WAN Manager. When the certificate installation is complete, refresh the browser page.
Enterprise (Auto)	Generate a certificate signing request (CSR), and automatically get it signed by an external certificate authority (CA) selected by your organization. This option requires configuring either EST (Enrollment over Secure Transport) or SCEP (Simple Certificate Enrollment Protocol), which are certificate enrollment protocols. As described earlier, configure these in **Administration** > **Settings** > **Certificate settings** > **Enterprise certificate settings**. When the certificate installation is complete, refresh the browser page.
Enterprise (Manual)	Generate a certificate signing request (CSR), to be signed by an external certificate authority (CA) selected by your organization. After getting the certificate signed, import it into SD-WAN Manager. When the certificate installation is complete, refresh the browser page. In a multitenant environment, we recommend that during this process, tenants enter their organization's preferred DNS server name in the SAN DNS names field.