Cisco Catalyst SD-WAN Certificate Management Guide, Releases 26.x and Later

Cisco SD-WAN
Updated June 8, 2026

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

1 Certificate Management

Topics:

Feature history of certificate management

Developments in certificate management, by release.

Developments in certificate management, by release.

Table 1: Feature history

Feature name	Release information	Feature description
Certificate Revocation	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature revokes enterprise certificates from devices based on a certificate revocation list that SD-WAN Manager obtains from a root certificate authority.
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 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.
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 SD-WAN Manager-signed certificates to Cisco PKI as the default certificate method for virtual routers to enhance security and reliability.
Web server certificate installation	Cisco Catalyst SD-WAN Control Components Release 26.1.1.1	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

Managing certificates in SD-WAN Manager

Describes the information that SD-WAN Manager provides about certificates, and the controls for managing them.

Information and controls for managing certificates in SD-WAN Manager, in **Configuration** > **Certificates**.

Information or control	Description
Top bar	On the left are the menu icon, for expanding and collapsing the SD-WAN Manager menu, and the 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 SD-WAN Control Components in the fabric and manage the serial numbers in the file.
	- **Send to Controllers**: Send the WAN edge router chassis and serial numbers to the controllers in the network.
	- **Validate** column: The certificate status can be:
	  - Valid (shown in green): Device certificate is valid.
	  - Staging (shown in yellow): Device is in the staging state.
	  - Invalid (shown in red): Device certificate is not valid.

Information or control	Description

Controllers tab	Install certificates and download the device serial numbers to the SD-WAN Validator.
	• Send to SD-WAN Validator: Send the controller serial numbers to the 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.
	
	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.

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.

Stage a WAN edge device

Procedure for staging a device.

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

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

1. In the **WAN Edge List** tab, select a device to stage.
2. In the **Validate** column, select **Staging**.
3. Select **OK** to confirm the move to the staging state.
4. Select **Send to Controllers** in the upper left corner to sync the WAN edge authorized serial number file with the SD-WAN Controllers. SD-WAN Manager shows the status of the push operation.
5. To advance the device from staging to production, validate the device.

Invalidate a device

Procedure to invalidate WAN edge devices.

1. In the **WAN Edge List** tab, select the device to invalidate.
2. In the **Validate** column, select **Invalid**.
3. Select **OK** to confirm the move to the invalid state.
4. Repeat the steps for each device you wish to invalidate.
5. Select the **Send to Controllers** button in the upper left corner to send the chassis and serial numbers of the validated devices to the SD-WAN Controllers in the network. SD-WAN Manager shows the status of the push operation.

Send SD-WAN Controller serial numbers to the SD-WAN Validator

Procedure to send the controller serial numbers to the SD-WAN Validator.

To determine which SD-WAN Controllers in the fabric are valid, SD-WAN Validator keeps a list of the SD-WAN Controller serial numbers. SD-WAN Manager learns these serial numbers during the certificate-generation process.

1. In the **Control Components** tab, check the certificate status bar. If the **Send to Controllers** check mark is green, all serial numbers have already been sent to the SD-WAN Validator. If it is gray, you can send one or more serial numbers to the SD-WAN Validator.
2. Select **Send to Validator** in the **Control Components** tab. The SD-WAN Controller's serial number and the UUIDs of the validated routers are sent to the SD-WAN Validator. If all serial numbers have been sent, when you select **Send to Validator**, an error message is displayed. To resend an SD-WAN Controller's serial number, first select the device and then select **Invalid** in the Validity column.
3. Optionally, after the serial numbers have been sent, select the **Tasks** icon in the SD-WAN Manager toolbar to display a log of the file download and other recent activities.

Install a signed certificate

Procedure to manually install a 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 SD-WAN Control Components.

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 **Control Components** tab, select **Install Certificate**.
2. In **Install Certificate**, select a file, or copy and paste the certificate text.
3. Select **Install** to install the certificate on the device. The certificate contains information that identifies the SD-WAN Controller.
4. Repeat the steps to install additional certificates.

Export a root certificate

Describes how to export a root certificate, saving it as a file.

1. In the **Control Components** tab, select **Export Root Certificate**.
2. In **Export Root Certificate**, select **Download** to export the root certificate to a file.
3. Click **Close**.

View a certificate signing request

Procedure to view a certificate signing request.

1. In the WAN edge list or the **Control Components** tab, select a device.
2. Select the **More Actions** icon to the right of the row, and choose **View CSR** to view the certificate signing request (CSR).

View a device certificate signing request

Procedure to view a device certificate signing request.

1. In the WAN edge list or the **Control Components** tab, select a device.
2. Select the **More Actions** icon to the right of the row, and choose **View Device CSR** to view the certificate signing request (CSR).

   For a device for which a trustpoint has been configured, selecting **More Actions** gives three options:

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

> **Note**
>
> SD-WAN Manager generates a certificate expiration alarm only if device certificate is installed through SD-WAN Manager. If you install a certificate manually, SD-WAN Manager does not generate an alarm for certificate expiration.

View a certificate

Procedure to view a certificate.

1. In the **Control Components** tab, select a device.
2. Select the **More Actions** icon in the row and choose **View Certificate**.

Generating a certificate signing request

Procedure to generate a certificate signing request.

These procedures describe the process of generating CSRs.

Generate an SD-WAN Control Component certificate signing request, through 20.16.x

Procedure to generate an SD-WAN Control Component certificate signing request.

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

1. From the Cisco SD-WAN Manager menu, select **Configuration** > **Certificates**.
2. Select **Control Components**.
3. For the desired controller, select **...** and choose **Generate CSR**.

   The **Generate CSR** page is displayed.
4. In the **Generate CSR** window, select **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 steps to generate a CSR for another SD-WAN Control Component.

Generate a feature certificate signing request, through 20.16.x

Procedure to generate a feature certificate signing request.

> **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

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

   This displays the **Generate Feature CSR** page.
4. On the **Generate Feature CSR** page, select **OK** to continue with the generation of a feature CSR. This step authenticates the device trustpoint that has been set and extracts the CSR from the device.
5. Repeat the steps for each device for which you are generating a CSR.

Generate a device certificate signing request, through 20.16.x

Procedure to generate a Cisco WAN edge device certificate signing request.

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

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

   This displays the **Renew Device CSR** page.
4. On the **Renew Device CSR** page, select **OK** to continue with the generation of a new CSR.

> **Note**
>
> Cisco vManage Release 20.9.1 and later releases: Selecting **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 these: Selecting **Renew Device CSR** generates a CSR using the existing key pair.

Reset the RSA key pair

Procedure to reset the RSA key pair.

1. In the **Control Components** tab, select a device.
2. Select the **More Actions** icon tand select **Reset RSA**.
3. Select **OK** to confirm resetting of the device's RSA key and to generate a new CSR with new public or private keys.

Invalidate an SD-WAN Control Component

Procedure to invalidate a device.

When invalidating the last remaining SD-WAN Validator or SD-WAN Controller in a fabric, 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.

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.
3. Adjacent to the SD-WAN Control Component instance, select **...** and choose **Invalidate**.

Invalidate a device certificate

Procedure to invalidate a device certificate.

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

View a log of certificate activities

Procedure to view the log of certificate activities.

1. Select the **Tasks** icon located in the SD-WAN Manager toolbar. SD-WAN Manager displays a list of all running tasks, and the total number of successes and failures.
2. Select a row to see details of a task. SD-WAN Manager 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

Procedure to 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. Select the **Control Components** tab.
3. For the desired device, select **...** and choose **View Certificate** to view the installed certificate.

Revoking certificates

Procedure to revoke designated certificates from devices that are included in a certificate revocation list (CRL), which is obtained from a root certificate authority (CA).

An enterprise certificate is a secure authentication framework that:

- allows organizations to use their own private certificate signing authority instead of public authorities, and
- authenticates and establishes secure communication between SD-WAN devices within the fabric.

If you are using enterprise certificates with Cisco Catalyst SD-WAN, you can enable 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.

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

When you enable certificate revocation and provide the URL of the CRL to SD-WAN Manager, 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, SD-WAN Validators, and 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 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 revoking certificates

Describes restrictions to be aware of while revoking certificates.

These are restrictions that apply to revoking certificates.

Disabled by default

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

Applicable only if you are using an enterprise CA to sign certificates

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

Connecting to a server to retrieve a CRL

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

VPN 512 support

From Cisco vManage Release 20.11.1, connections through the VPN 512 are supported.

Revoke certificates

Procedure to revoke enterprise certificates from devices based on a certificate revocation list.

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

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. On the **Administration Settings** page, select **Edit** adjacent to **Certificate Revocation List**.

   The certificate revocation options appear.

3. Select **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 SD-WAN Manager retrieves the CRL from your secure server and revokes the certificates that the CRL designates.

   Possible values: 1 to 24

   Default retrieval interval: 1 hour

6. Select **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

A Cisco SD-WAN public key infrastructure (PKI) certificate is a digital certificate that provides automated certificate management by linking certificates to a Smart Account and Virtual Account, and supports a variety of security protocols.

A Cisco SD-WAN public key infrastructure (PKI) certificate is a digital certificate that:

- provides automated certificate management by linking certificates to a Smart Account and Virtual Account, and
- supports a variety of 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, 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 SD-WAN Controllers continue to support a SD-WAN Manager-signed certificate if it is already enabled. However, when the certificates are renewed, the SD-WAN Controllers have a PKI certificate by default.

Comparison with other certificates

In contrast with Symantec/Digicert certificates, 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 supporting PKI certificates

These devices support using 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

Renew a certificate

Procedure to renew a certificate.

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Select **WAN Edge List**.
3. For the desired SD-WAN Controller, select **...** and choose **Renew CSR**.

   The **Renew CSR** opens.

The certificates are renewed in this order:

1. Cisco SD-WAN Manager
2. Cisco SD-WAN Validator
3. Cisco SD-WAN Controller
4. Cisco IOS XE Catalyst SD-WAN device

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

Describes how SD-WAN Manager stages and tests new edge device certificates with the SD-WAN Validator before installation, completing the install only if the staged certificate successfully establishes a validated control connection.

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.

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.

Install a web server certificate

Procedure to install a web server certificate.

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**.

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

2 Certificate Management for Cisco SD-WAN Control Components

Topics:

SD-WAN Control Components certificate management feature history

Describes developments in SD-WAN Control Components certificate management, by release.

Developments in SD-WAN Control Components certificate management, by release.

Feature Name	Release Information	Description
SD-WAN Control Components Certificate Management workflow	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Control Components Release 20.18.1	The Control Components Certificate Management workflow updates the authentication certificates for SD-WAN Control Components in the fabric. This is useful for updating certificates before they expire.

Control Components Certificate Management workflow

Describes the Control Components Certificate Management Workflow, a step-by-step workflow that updates the authentication certificates for SD-WAN Control Components.

The Control Components Certificate Management Workflow in Cisco SD-WAN Manager is a step-by-step interactive procedure (called a workflow) that updates the authentication certificates for SD-WAN Control Components.

Cisco Catalyst SD-WAN uses authentication certificates to authenticate components when establishing control connections between SD-WAN Control Components, or between SD-WAN Control Components and edge devices. SD-WAN Manager can manage the certificates installed on components in the network:

- SD-WAN Control Components
- WAN edge devices

Certificates expire and require renewal. Use this SD-WAN Manager workflow to renew the certificates for SD-WAN Control Components.

Expired certificates

From SD-WAN Control Components 20.18.1, control connections between SD-WAN Control Components and edge devices remain operational even when the certificates on SD-WAN Control Components have expired. Control connections may also successfully re-establish after being manually cleared, including connections to SD-WAN Controllers with expired certificates. This maintains the functionality of the fabric.

Supported environments for the Control Components Certificate Management workflow

Describes which Cisco Catalyst SD-WAN environments support the Control Components Certificate Management workflow.

Describes which Cisco Catalyst SD-WAN environments support this feature.

The workflow applies to Cisco Catalyst SD-WAN environments in which you manage the SD-WAN Control Components.

Supported components for the Control Components Certificate Management workflow

Describes which SD-WAN Control Components support this feature.

Describes which SD-WAN Control Components support this feature.

- Cisco SD-WAN Manager
- Cisco SD-WAN Controller

- Cisco SD-WAN Validator

Renew certificates using the Control Components Certificate Management workflow

Procedure to renew certificates using the Control Components Certificate Management workflow.

The Control Components Certificate Management workflow provides two methods:

- **Auto**: For each selected SD-WAN Control Component, SD-WAN Manager generates a certificate signing request (CSR), sends the CSR to the certificate authority (CA) for signing, then installs the signed certificate on the component.

  The **Auto** option is available if you have selected one of the Cisco PKI, EST, or SCEP options in **Administration** > **Settings** > **Certificate settings**.

- **Manual**: For each selected SD-WAN Control Component, SD-WAN Manager generates a certificate signing request (CSR) for you to download. Then you manually handle the certificate signing and re-upload the signed certificate. The workflow then installs the signed certificate on the component.

For the automatic certificate signing option that occurs in the workflow, two prerequisites apply. Without these, only a manual signing option is available in the workflow. Here are the prerequisites:

- Smart Account and Virtual Account

  In Cisco Catalyst SD-WAN Manager Release 20.18.1 and earlier, enter Smart Account and Virtual Account details in Cisco SD-WAN Manager.

  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials**.
  2. Enter your Smart Account or Virtual Account credentials in the **Username** and **Password** fields.

- Registering Plug-and-Play

  From Cisco Catalyst SD-WAN Manager Release 20.18.2, service providers in a multitenant environment and tenant in a single-tenant environment must register the Plug-and-Play service.

- Certificate signing by Cisco

  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Certificate settings**.
  2. Click **Control Components**.
  3. Change **Certificate Signing by** to **Cisco**.

1. Do one of these to launch the Control Components Certificate Management workflow:
   - Launch from the workflow library.
     a. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
     b. Launch the Control Components Certificate Management workflow.
   - Launch from the **Control Components** page.
     a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components**.
     b. Click **Certificate management** to launch the Control Components Certificate Management workflow.
2. Choose **Auto** or **Manual**, select the desired SD-WAN Control Components, and proceed according to the instructions in the workflow.

   For the **Manual** option:

- File formats

  If you use the **Manual** option, which requires you to complete the signing for each certificate manually, outside of SD-WAN Manager, add the signed certificates to a single archive file to upload at the required step. The workflow supports these file formats for upload:

  - zip
  - pem
  - crt
  - cer

  If you are renewing certificates for multiple SD-WAN Control Components simultaneously, we recommend using the zip format so that you can combine all certificates into a single zip file to upload.

- Signed certificates

  If you use the **Manual** option, which requires you to complete the signing for each certificate manually, the archive file that you upload with the signed certificates must include a signed certificate for each selected SD-WAN Control Component. If the uploaded file does not contain signed certificates for each, the workflow does not proceed.

3 Certificate Management for Edge Devices

Topics:

Feature history for edge device certificate management

Describes developments in WAN edge device certificate management, by release.

Developments in WAN edge device certificate management, by release.

Table 2: Feature history

Feature Name	Release Information	Description
WAN Edge Device Certificate Management Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	The WAN edge device certificate management workflow updates the authentication certificates for edge devices in the fabric. This is useful for updating certificates before they expire.

WAN edge device certificate management workflow

Describes the WAN edge device certificate management workflow, which is an interactive process in SD-WAN Manager for updating authentication certificates on edge devices to maintain secure network communication.

The WAN edge device certificate management workflow is a step-by-step interactive procedure in SD-WAN Manager that updates authentication certificates for edge devices in the network.

- Used to renew authentication certificates for WAN edge devices.
- Required when certificates expire and need renewal, and
- Ensures secure communication between edge devices and other network components in the fabric.

The WAN edge device certificate management workflow in SD-WAN Manager is essential for maintaining the validity of authentication certificates on edge devices.

For example, when a certificate on a WAN edge device is about to expire, an administrator can use the SD-WAN Manager workflow to initiate the renewal process, ensuring uninterrupted secure communication within the network.

Supported components

The workflow supports Cisco IOS XE Catalyst SD-WAN devices and Cisco edge devices.

Supported solutions

The workflow applies to WAN edge devices in the SD-WAN or SD-Routing solutions.

Supported solutions for the edge device certificate management workflow

Describes which Cisco solutions support the edge device certificate management workflow.

Describes which Cisco solutions support the edge device certificate management workflow.

The workflow applies to WAN edge devices in the

- SD-WAN solution, or
- SD-Routing solution

Supported components for the edge device certificate management workflow

Describes which network components support the edge device certificate management workflow.

Describes which network components support the edge device certificate management workflow.

- Cisco IOS XE Catalyst SD-WAN devices
- Cisco vEdge devices

Renew certificates using the edge device certificate management workflow

Describes how to renew certificates for WAN edge devices using the certificate management workflow, including both automatic and manual signing options, and required prerequisites for each method.

The WAN Edges Certificate Management workflow provides two methods:

- Auto: For each selected WAN edge device,SD-WAN Manager generates a certificate signing request (CSR), sends the CSR to the certificate authority (CA) for signing, then installs the signed certificate on the device.
- Manual: For each selected WAN edge device,SD-WAN Manager generates a certificate signing request (CSR) for you to download. Then you manually handle the certificate signing and re-upload the signed certificate. The workflow then installs the signed certificate on the device.

For the automatic certificate signing option in the workflow, two prerequisites apply. If these are not met, manual signing option is available in the workflow. The prerequisites for automatic certificate signing are:

- Smart Account and Virtual Account

  In SD-WAN Manager 20.18.1 and earlier, enter Smart Account and Virtual Account details in SD-WAN Manager.

  1. From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials** .
  2. Enter your Smart Account or Virtual Account credentials in the **Username** and **Password** fields.

- Register Plug-and-Play

  From SD-WAN Manager 20.18.2, service providers in a multitenant environment and tenant in a single-tenant environment must register the Plug-and-Play service.

- Certificate signing by Cisco

  1. From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Certificate settings**.
  2. Select **WAN Edges for 20.18.x and above**.
  3. Change **Certificate Signing by** to **Cisco**.

Follow these steps renew certificates using the edge device certificate management workflow.

1. From the SD-WAN Manager menu, choose **Workflows** > **Workflow Library** .
2. Launch the WAN Edges Certificate Management workflow.
3. Choose **Auto** or **Manual** , select the desired WAN edge devices, and proceed according to the instructions in the workflow.

   The workflow lists each WAN edge device, and the certificate information for each, including expiration date.

   - File formats

     If you use the **Manual** option, which requires you to complete the signing for each certificate manually, outside of SD-WAN Manager , add the signed certificates to a single archive file to upload at the required step. The workflow supports these file formats for upload:

- `zip`
- `pem`
- `crt`
- `cer`

  If you are renewing certificates for multiple devices simultaneously, we recommend using the zip format so that you can combine all certificates into a single zip file to upload.

- Signed certificates

  If you use the **Manual** option, which requires you to complete the signing for each certificate manually, the archive file that you upload with the signed certificates must include a signed certificate for each selected device. If the uploaded file does not contain signed certificates for each, the workflow does not proceed.

4 Third-party Certificate Authority

Topics:

Third-party Certificate Authority

Describes developments in the support for a third-party certificate authority, by release.

Developments in the support for a third-party certificate authority, by release.

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.

Third-party certificate authority certificates for edge devices

Describes the use of a third-party certificate authority for devices in a Cisco Catalyst SD-WAN fabric.

A third-party certificate authority (CA) used for devices in a Cisco Catalyst SD-WAN fabric is a trusted external entity that issues digital certificates to authenticate device identities and secure communications.

A third-party CA certificate is a digital certificate that

- authenticates device identities for secure communications,
- establishes and verifies secure connections between devices by validating server identities, and
- requires more manual certificate signing and installation processes, unlike Cisco PKI certificates, which can be automated.

Initial setup

SD-WAN Manager permits uploading third party certificates to devices during their integration with the fabric. This is only available during the initial setup, when devices are installed and control connections are established.

Certificate upload

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, SD-WAN Manager provides a method for uploading certificates, not requiring the use of CLI commands. It supports CA certificate uploads even after device setup.

Authenticating server identities

The CA certificates authenticate the server identities and prevent unauthorized access. 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 SD-WAN Manager, devices use the certificate information from the configuration group parcels to verify and authenticate the connections it establishes with servers across a network, improving the security and integrity of your network traffic.

Devices that support third-party certificates

Describes which devices support third-party certificates.

Devices that support third-party certificates:

Cisco IOS XE Catalyst SD-WAN devices

Prerequisites for third-party certificate authority certificates

Describes prerequisites for using third-party CA certificates.

Prerequisites for uploading third-party CA certificates.

SD-WAN Manager release

SD-WAN Manager release: Cisco Catalyst SD-WAN Manager Release 20.13.1 and later

Device software release

Cisco IOS XE Catalyst SD-WAN device software release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and later

Restrictions for third-party certificate authority certificates

Describes the restrictions for using third-party certificate authority certificates.

List of restrictions for using third-party certificate authority certificates

PEM encoded certificate files.

Supports only PEM encoded certificate files.

Maximum certificate file size

Maximum certificate file size: 10 MB

Multitenancy

In a multitenancy environment, only a tenant can upload and manage CA certificates.

> **Note**
>
> When you log in into SD-WAN Manager as a provider, you can't upload or manage CA certificates.

Upload third-party certificate authority certificates

Procedure for uploading third-party certificate authority certificates.

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

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

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

Delete third-party certificate authority certificates

Procedure to delete third-party certificate authority certificates.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
2. Select the **CA Cert** tab.
3. In the **Device Group** table, select the CA certificate to delete.
4. Select **Delete**.

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

Configure devices to use third-party certificate authority certificates, using a configuration group

Procedure for configuring devices to use third-party certificate authority certificates, using a configuration group.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. For a configuration group, under **System Profile**, select **Add Feature**.
3. In the **Add Feature** pane, choose **CA Certificate**.
4. 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	Select **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.

5. Select **Save**.

6. Deploy the devices associated to the configuration group.

When you modify a certificate from the **Device Group** table, the changes are not be reflected on the device. This is because of the certificate's association with a TrustPoint. To update the certificate, remove the existing TrustPoint that contains the certificate information. Then create a new TrustPoint and add the certificate to it. 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, manually delete and then save the changes to the TrustPoint.

Revoke third-party certificate authority certificates

Procedure to revoke third-party certificate authority certificates.

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

Renew third-party certificate authority certificates

Procedure to renew third-party certificate authority certificates.

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

Monitoring third-party certificate authority certificates

Provides information about monitoring third-party certificate authority certificates.

Methods of monitoring third-party certificate authority certificates.

Monitor CA Certificate Installation

After the third-party CA certificate installation is complete, the device sends event logs to 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`.

Track a third-party certificate authority certificate

Procedure to track a third-party certificate authority certificate.

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

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

5 Expired certificate indication and quarantine

Topics:

Feature history for expired certificate indication and quarantine

Describes the development of the expired certificate indication and quarantine feature, by release.

Development of expired certificate quarantine, by release.

Table 5: Feature history

Feature name	Release information	Feature description
Expired Certificate Indication and Quarantine	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Control Components Release 20.16.1	Cisco SD-WAN Manager indicates when devices or Cisco Catalyst SD-WAN Control Components have expired certificates. Additionally, you can quarantine all edge devices that have expired certificates. Quarantine places devices into the staging status. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.

Expired certificate indication and quarantine

Describes how SD-WAN Manager checks devices for expired certificates and quarantines devices that require a certificate renewal.

Describes how SD-WAN Manager checks devices for expired certificates and quarantines devices that require a certificate renewal.

Indication of expired certificates

A digital certificate is used to authenticate devices in the overlay network. After authentication, devices and Cisco Catalyst SD-WAN Control Components can establish secure sessions with one another. A certificate is issued by a certificate authority and has an expiration date.

Every several minutes, SD-WAN Manager checks the devices and Cisco Catalyst SD-WAN Control Components in the network for expired certificates. If it detects any expired certificates, SD-WAN Manager displays a banner with a link to the **Configuration** > **Certificates** > **WAN Edges** page or **Configuration** > **Certificates** > **Control Components** page to show the details of which devices or components require certificate renewal.

> **Note**
>
> Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the SD-WAN Manager UI parses certificate expiration dates by using the **expirationdatelong** command, which uses the epoch time standard, ensuring consistency across all time zones.

Device quarantine

Quarantine refers to placing devices into a staging state. Quarantined devices keep their control connections to SD-WAN Control Components, but do not handle data plane traffic.

You can quarantine devices that have expired certificates. Refer to Enable quarantining devices with expired certificates on page 39.

Quarantining devices with expired certificates enforces the requirement to renew an expired certificate. Removing network elements with expired certificates may be necessary to comply with an organization's network security requirements.

This table shows which devices are subject to automatic quarantine when the quarantine feature is enabled.

Table 6: Automatic quarantine for expired certificate

Device or SD-WAN Control Component	Automatic quarantine when quarantine enabled?
Hardware devices using a certificate	Yes
Hardware devices using an on-box trusted platform module (TPM) secure unique device identifier (SUDI) certificate	No
Software devices	Yes
SD-WAN Control Components	No

Multitenancy

In a multitenancy scenario, enabling quarantine for expired certificates is possible only at the provider level and applies to all tenants.

Enable quarantining devices with expired certificates

Procedure to enable quarantining devices the SD-WAN Manager detects to have expired certificates.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Select **Device Quarantine**.
3. Enable device quarantine.

View and remedy devices in expired certificate quarantine

View and remedy devices that SD-WAN Manager has placed in quarantine for an expired certificate.

Enable quarantine for expired certificates. Refer to Enable quarantining devices with expired certificates on page 39.

1. Open the **Configuration** > **Certificates** > **WAN Edges** page to show a table with details of which devices require certificate renewal.

   If SD-WAN Manager is displaying a banner message indicating that one or more devices are quarantined for expired certificates, select the link in the banner message to open the page.

   In the table, an exclamation point icon indicates a problem with a device. Hover over the icon to display the details of the problem, such as an expired certificate. If a device is quarantined, the **Validate** column for the device shows staging.

2. To remove a device from quarantine, renew its certificate.

6 Certificate Revocation List-based Quarantine

Topics:

Feature history of certificate revocation list-based quarantine

Describes the development of certificate revocation list (CRL)-based quarantine, by release.

Development of certificate revocation list (CRL)-based quarantine, by release.

Table 7: Feature history

Feature Name	Release Information	Feature Description
CRL-based Quarantine	Cisco vManage Release 20.11.1	You can quarantine WAN edge devices based on a certificate revocation list that SD-WAN Manager receives from a certificate authority.

Certificate revocation list-based quarantine

Describes certificate revocation list (CRL)-based quarantine, a security mechanism that quarantines devices whose certificates have been revoked and are listed in a certificate revocation list, moving the devices to a staging mode.

Certificate revocation list (CRL)-based quarantine is a security mechanism that

- quarantines devices whose certificates have been revoked and are listed in a certificate revocation list received from a certificate authority,
- moves quarantined devices into a staging mode, and
- generates notifications for quarantined devices to alert administrators.

How CRL-based quarantine works

When the CRL-based quarantine feature is enabled, SD-WAN Manager quarantines devices whose certificates are included in a periodically updated certificate revocation list (CRL), which it receives from a certificate authority (CA).

The feature is disabled by default.

1. At a defined interval, SD-WAN Manager polls a CRL server for the latest CRL, which contains serial numbers of certificates.

   Note

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

2. If any serial numbers match the certificates of devices in the fabric, SD-WAN Manager proceeds to quarantine the devices.
3. SD-WAN Manager moves the devices requiring quarantine to a staging mode. This mode shuts down data traffic on the device, but does not remove the certificate from the device. Keeping the certificate on the device allows it to continue its control connection to SD-WAN Manager.
4. SD-WAN Manager generates notifications for the device being quarantined.

Restrictions for certificate revocation list-based quarantine

Describes restrictions for certificate revocation list-based quarantine.

This is a list of restrictions for certificate revocation list (CRL)-based quarantine.

Enterprise certificate authority requirement

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.

CRL-based quarantine and certificate revocation

You cannot enable the certificate revocation and CRL-based quarantine option at the same time.

Disable the CRL to switch from certificate revocation to quarantine or quarantine to certificate revocation.

Configure certificate revocation list-based quarantine

Procedure to quarantine devices based on a certificate revocation list.

By default, the certificate revocation list (CRL)-based quarantine feature is disabled.

- From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**. Select an option 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.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. On the **Administration Settings** page, select **Edit** near **Certificate Revocation List**.
3. Select **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, for retrieving the CRL.

   Possible values: 1 to 24

   Default: 24 hours
6. Select **VPN 0** or **VPN 512**. SD-WAN Manager connects to a server to retrieve the CRL through the VPN 0 or VPN 512 interface.
7. Select **Save**.

   At the configured interval, SD-WAN Manager polls the CRL server for the latest CRL. It uses this list to determine whether to quarantine devices.

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.

7 Root Certificate Authority Certificates

Topics:

Feature history for root certificate authority certificates

Describes developments in root certificate authority certificate support, by release.

Developments in root certificate authority certificate support, by release.

Table 8: Feature history

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	Add and manage root certificate authority (CA) certificates.

Add root certificate authority certificates

Procedure for adding root CA certificates.

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Select **Modify Root CA**.
3. In the **Root Certificate** field, paste in the text of a certificate, or select **Select a File** to load a certificate from a file.
4. Select **Add**.

   The new certificate appears in the certificate table. The **Recent Status** column indicates that the certificate has not yet been installed.
5. Select **Next** and review the details of any certificates that have not been installed.
6. Select **Save** to install the certificates.

   The new certificate appears in the certificate table.

View root certificate authority certificates

Procedure for viewing a root CA certificate in SD-WAN Manager.

1. In Cisco SD-WAN Manager, choose **Administration** > **Root CA Management**.
2. Optionally, 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, select **More Actions** (**...**) and choose **View**.

   SD-WAN Manager shows the certificate and its details.

Delete root certificate authority certificates

Procedure to delete a root CA certificate in SD-WAN Manager.

> **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.

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

8 Enterprise Certificates

Topics:

Feature history of enterprise certificates

Describes developments in enterprise certificate support, by release.

Developments in enterprise certificate support, by release.

Table 9: Feature history

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.
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.
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.

Enterprise certificates

Describes enterprise certificate support in Cisco Catalyst SD-WAN.

An enterprise certificate is a digital certificate that

- allows organizations to use their own private certificate signing authority instead of relying on public certificate authorities,

- authenticates the identity of Cisco Catalyst SD-WAN components such as SD-WAN Controllers and edge devices, and
- enables secure sessions between authenticated devices within the overlay network.

About enterprise certificate support

Enterprise certificates allow organizations to use their own private certificate signing authority rather than having to rely on public certificate signing authorities.

Enterprise certificate support was introduced in Cisco IOS XE SD-WAN Release 16.11.1 and Cisco SD-WAN Release 19.1, replacing the previous controller certificate authorization method. Enterprise certificates support features such as custom certificate properties and RSA key lengths from 2048 to 4096 bits. They are supported on Cisco SD-WAN Manager, Validator, Controller, and most hardware WAN edge routers.

Certificates and authorized serial number files must be installed on SD-WAN Control Components to validate and authenticate the overlay network components, ensuring operational security.

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

Setup

The goal of setting up certificates in the fabric is to install signed certificates on the SD-WAN Control Components and edge devices in the fabric. This allows the network components in the fabric to validate and authenticate each other, which allows them to establish secure connections between each other. This enables the fabric to become operational.

Device support for enterprise certificates

Describes the devices that support enterprise certificates.

Lists 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

Restrictions for enterprise certificates

Describes restrictions for enterprise certificate support in Cisco Catalyst SD-WAN.

Restrictions for enterprise certificate support.

Certificate encodings

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

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.

Device reset and upgrade

Resetting a WAN edge device removes the enterprise root certificate. After the reset, you have to re-install the certificate.

Upgrading a WAN edge device does not affect the enterprise root certificate.

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, and Cisco Catalyst SD-WAN Control Components Release 20.13.1 and later, 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.

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.

Configure enterprise certificates

Procedure for configuring enterprise certificates.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Hardware WAN Edge Certificate Authorization**.
2. Select **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, select **Set CSR Properties** and configure the following properties.

Property	Description
Domain Name	Network domain name. Do not exceed 17 characters.

Property	Description
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.
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 SD-WAN Control Components 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 is shown in the text box.

5. Select **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 devices list and select **Upload**.
9. On the **Configuration** > **Certificates** page, select **...** and choose an action:

Action	Description
View Enterprise CSR (certificate signing request)	Copy the CSR and sign it using the enterprise root certificate, and upload the signed certificate on SD-WAN Manager using the install certificate operation. 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 expiration data on the **Configuration** > **Certificates** page. **Note** The certificates that you install on devices in the Cisco Catalyst SD-WAN fabric 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	Removes the enterprise certificate from the device and moves it back to prestaging. The device has only SD-WAN Validator and SD-WAN Manager controls up.

For a WAN edge device, select **...** and choose an action:

Action	Description
View Feature CSR	• Copy the CSR available from the device. • Sign the certificate using the enterprise root certificate from a certifying authority. • Upload the signed certificate on SD-WAN Manager using the **Install Feature Certificate** operation. 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.

Action	Description
View Feature Certificate	After you install the feature certificate, you can view the feature certificate and download it.
Revoke Feature Certificate	Removes the feature certificate or trustpoint information from the WAN edge 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 the 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. Select **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.

Use an enterprise certificate with SD-WAN Control Components

Procedure for using an enterprise certificate with SD-WAN Control Components.

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

   Note

   In a multitenant 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 multitenant 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.

  From Cisco Catalyst SD-WAN Manager Release 20.12.1, the system Organization Name cannot contain a comma during the device configuration.
- **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 select **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.
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.

9 Automated certificate management

Topics:

Provides information about automated certificate management capabilities and features.

Feature history for automated certificate management

Describes developments in automated certificate management, by release.

Developments in automated certificate management, by release.

Table 10: Feature history

Feature Name	Release Information	Description
Automated Certificate Management with EST and SCEP	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	With this feature, EST (Enrollment over Secure Transport) and SCEP (Simple Certificate Enrollment Protocol) helps automate the process of enrolling and renewing certificates on devices and services using Cisco SD-WAN Manager.

Automated certificate management

Describes the automated certificate management using EST and SCEP protocols for WAN edge devices.

Automated certificate management on Cisco SD-WAN Manager is a system that

- uses protocols such as EST and SCEP to automate certificate enrollment and renewal for WAN edge devices
- introduces enterprise certificate settings to unify certificate management across controller components, hardware WAN edges, and cloud WAN edges, and
- requires manual intervention to initiate renewal processes when certificate expiry alarms are triggered.

Certificate management functionality

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

In Cisco SD-WAN Manager automatic renewal of certificates using SCEP and EST configurations occurs only during the initial device onboarding or when migrating from a hardware SUDI certificate to an enterprise certificate. For subsequent renewals, manual intervention is required to initiate the process when a certificate expiry alarm is triggered in Cisco SD-WAN Manager. Once renewal is manually initiated, the system automatically manages the enrollment and installation of the new certificates. For more information, see Edge device certificate management .

Certificate management with Cisco SD-WAN Manager as a fabric client

Cisco SD-WAN Manager functions as a fabric client that:

- supports SCEP and EST protocols to facilitate certificate enrollment and renewal for devices
- enables independent certificate management on Cisco SD-WAN control components and WAN edge devices, and
- enhances network security and operational flexibility.

Prerequisites for automated certificate management on CA servers

Describes prerequisites for configuring automated certificate management on CA servers, including VPN reachability, encryption requirements, and protocol configurations.
System requirements and reachability

- Based on the chosen VPN (0 or 512), ensure that a route to the CA server is added, or that the CA server is reachable from the selected VPN.
- Ensure that the minimum key size for certificates is 2048 bits or higher in CA servers.

Encryption algorithm requirements

For Cisco SD-WAN Controllers, to renew certificates by configuring SCEP, the CA server should support encryption algorithm higher than triple DES.

EST configurations

Configure EST enrollment settings to ensure proper certificate management.

- Ensure that Cisco SD-WAN Manager enrolls through the EST URL and EST is enabled on the CA. Any certificate requested from Cisco SD-WAN Manager may include custom Common Name (CN) and Organizational Unit (OU) values. The CA should be configured not to override these custom values.
- Configure a username and password for EST enrollment if configured on CA server.
- When configuring EST, you must provide the hostname or IP address that matches the digital certificate of the server. Cisco SD-WAN Manager uses hostname verification in EST client.

SCEP configurations

Configure SCEP protocol settings on the CA server to support automated certificate enrollment.

- Allow SCEP protocol on the CA server.
- Configure a default SCEP alias if required.
- Enable enrollment through SCEP.
- Set a higher requests-per-minute limit on the CA server to accommodate anticipated enrollment volume.
- Ensure the minimum key size for certificates is 2048 bits or higher.
- Use an encryption algorithm stronger than triple DES.

Configure certificate settings

Procedure for configuring certificate authorization settings for SD-WAN Control Components, WAN edge devices, and enterprise certificates in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**
2. Choose **Certificate settings** .
   a) Configure the control component certificate authorization settings:

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise**

If you choose **Cisco PKI** configure the following parameters.

Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.

Field	Description
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the 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

b) Configure the WAN edge cloud certificate authorization settings

Table 11: WAN Edge Cloud Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise** • **Automated (Manager signed)** This option is available only if you are upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.

Field	Description
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the 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

c) Configure the hardware WAN edge certificate authorization settings

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI (SUDI certificate)** • **Enterprise**
If you choose **Enterprise** configure the following parameters.	

Field	Description
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the 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

d) You can configure the enterprise certificate settings in advance or when you configure the certificate authorization for the control components and the WAN edge devices.

Table 12: Enterprise Certificate Settings

Field	Description
Enrollment protocol type	Choose from one of the following: • **Manual** • **EST** • **SCEP** For EST and SCEP options the route type can be vpn 0 or vpn 512, through which you can allow reachability to the CA server.
If you choose **Manual** configure the following parameters.	
Enterprise root certificate	Choose **Select a file** to upload a root certificate authority file. The uploaded root certificate authority displays in the text box.

Field	Description
If you choose **EST** configure the following parameters.	
URL base	Enter the full EST URL seen on CA server for EST/SCEP certificate authorization server.
(Optional) **Username**	Enter the username for the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Password**	Enter the password to authenticate the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **CA Label**	Enter the CA label for EST CA server. Enter the same details here as per the configurations on the CA server. Use the following format to enter the CA label: • ip-address:port and enter alias, or • host-name:port and enter alias
Root CA certificate	Click **Select a file** to upload the root CA certificate of EST/SCEP CA server. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

Field	Description
Generate EST Client CSR	Enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the 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
Upload signed certificate file	Optionally, click **Select a file** to upload a signed certificate file. The signed certificate is obtained by signing the EST client CSR manually by CA.
If you choose **SCEP** configure the following parameters.	
URL base	Enter the full SCEP URL as configured on the certificate authorization server. With this url you can call endpoints for certificate enrollment and renewal.
(Optional) **Challenge password**	Enter the password for SCEP CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Root CA fingerprint**	Use the md5 fingerprint of root CA.
Root CA certificate	Click **Select a file** to upload the root CA certificate. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

3. Click **Save** .

Troubleshoot certificate management on CA server

Provides troubleshooting information for certificate management on CA server with error types, messages, root causes, and resolution steps.

This reference provides troubleshooting information for certificate management on CA server.

Error type	Error message	Pausible root cause	Troubleshooting steps
Internal server error	`https://<ca-server>/.well-known/est/<label>/simpleenroll HTTP Status Code: 500 500 Internal Server Error`	The CA server responds with a 500 error. High CPU or memory usage on the CA server.	• Check CA server logs for error details. • Check resource utilization on CA server. • Increase resource limits if necessary.
Timeout error	`Failed to get CSR signed for <device-id>, Failure reason - Read timed out HTTP Status Code: 0`	The API call to the CA server times out due to resource issues in CPU, memory, or enrollment rate limits on the CA server.	Increase resource limits or enrollment rate on the CA server.
Unauthorized Error	`Failed to get CSR signed for <device-id>, Failure reason - Simple Enroll: https://<ca-server>/.well-known/est/<label>/simpleenroll HTTP Status Code: 401`	• Authentication or configuration issue. • Incorrect or missing EST password. • EST client certificate lacks TLS authorization. • EST alias configurations are incorrect.	• Verify EST password in Cisco SD-WAN Manager and ensure that it matches CA server. • Check EST client certificate support for TLS authorization. • Check EST Alias configurations. • For SCEP, ensure correct challenge password is used.
EST Configuration Failure / Timeout	Loss of OMP connection with controller. Sync of root-CA certificate failed on controllers.	Failed Netconf, permission errors, or device/controller issues.	Check logs for issues on devices/controllers.