Revised: August 18, 2025

Certificate Management for SD-Routing Devices, Release 17.18.x

What's new

Cisco IOS XE	Feature name and description	Supported platforms
Cisco IOS XE 17.18.1a	Certificate Management for SD-Routing Devices This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrollment over Secure Transport) and SCEP (Simple Certificate Enrollment Protocol). The feature automates the enrollment, and renewal of certificates.	• Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco 1000 Series Integrated Services Routers • Cisco 4000 Integrated Services Router • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 1835 Rugged Router • Cisco Catalyst IR8340 Rugged Series Routers

Certificate management for SD-Routing devices

Certificate management for SD-Routing devices is a process that

- authenticates the identity of SD-WAN components before establishing control connections.
- establishes secure sessions between devices once authenticated.
- uses certificates generated from Cisco Catalyst SD-WAN Manager and installs them on control components.

From Cisco IOS XE 17.18.1a, Enterprise certificate, a new certificate authorization setting is being introduced to streamline certificate management processes. It is available for control components, hardware WAN edges, and software WAN edges.

This feature supports automated certificate management by using protocols like Enrollment over Secure Transport (EST) and Simple Certificate Enrollment Protocol (SCEP).

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.

Cisco SD-WAN Manager functions as a fabric client that supports SCEP and EST protocols. By enabling this setting, you can simplify certificate management processes and reduce manual intervention, resulting in more efficient and secure operations.

Prerequisites for certificate management on SD-Routing devices

The table below provides the details of key prerequisites.

VPN 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.

Encryption algorithm

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

Key size

Ensure that the minimum key size for certificates is 2048 bits or higher in CA servers.

Cisco PKI

To enable Cisco PKI for secure communication, you need to configure smart credentials.

EST configurations

- 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

- Allow SCEP protocol on the CA server.
- Configure a default SCEP alias if required.
- Enable enrollment through SCEP.
- Configure a challenge password for SCEP enrollment if configured on CA server.
- 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.

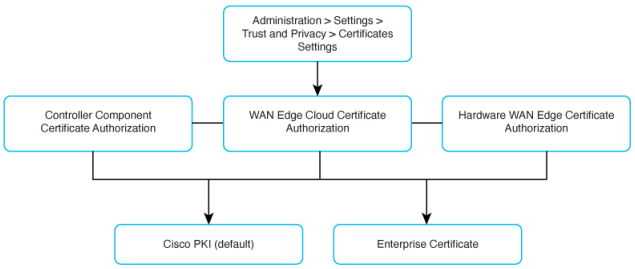
Enterprise certificates for Cisco SD-Routing devices

An Enterprise certificate is a type of digital certificate that

- allows organizations to use their own private certificate signing authority rather than relying on public certificate signing authorities,
- authenticates the identity of SD-WAN components, and
- establishes secure sessions between devices.

From **Cisco SD-WAN Manager** go to **Administration** > **Settings** > **Trust and Privacy** > **Certificates Settings** page to manage certificates.

Cisco Catalyst SD-WAN Manager provides multiple ways to authorize certificates.



The three components of Cisco Catalyst SD-WAN solution that provide device authentication are given below.

- **Controller Component Certificate Authorization** - 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 Cisco SD-WAN Manager instances, Cisco SD-WAN Validators, and Cisco SD-routing devices.
- **WAN Edge Cloud Certificate Authorization** - WAN Edge Cloud Certificate Authorization involves the process of ensuring that the certificates used by the cloud WAN Edge devices are authorized and valid.
- **Hardware WAN Edge Certificate Authorization** - Hardware WAN Edge Certificate Authorization involves the process of ensuring that the certificates used by the WAN Edge devices are authorized and valid.

Configure controller component certificate authorization

Follow these steps to configure controller component certificate authorization.

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Trust and Privacy** > **Certificates Settings** > **Controller Component Certificate Authorization**
Choose from:

- Cisco PKI is the default option. To continue using Cisco PKI, follow these steps.
  a. Select **Sync Root Certificate** to migrate the Cisco IOS XE Catalyst SD-Routing devices in Cisco SD-WAN Manager to Cisco PKI.
  b. Select the **validity period** from the drop-down list.
- Alternatively, if you prefer to use **Enterprise Certificate**, follow these steps.
  a. Click **Enterprise Certificate**.
  b. Click **Edit Settings**, to modify the settings. For more details, refer, *Configure enterprise certificate settings*.

c. If you want to specify custom certificate properties, click **Set CSR Properties** and configure the below parameters.

Parameter	Description
Domain Name	Network domain name
Organization	Organization name
Organizational Unit	Organizational unit name
Secondary Organization Unit	Secondary organizational Unit name
City	City name
State	State name
2-Letter Country Code	Email address
(Optional) Subject Alternative Name (SAN) DNS Names	You can configure multiple host names to use the same SSL certificate. Example, cisco.com and cisco2.com
(Optional) Subject Alternative Name (SAN) URIs	You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example, cisco.com and support.cisco.com

Step 2 Click **Save.**

Controller component certificate authorization is complete.

Configure WAN Edge Cloud certificate authorization

To authorize certificates for WAN Edge cloud devices.

From IOS XE 17.18 onwards, only Cisco PKI and Enterprise Certificate options are available. If you upgrade from an earlier release with vManage CA selected, that option will be visible but will be removed if you switch to another option.

Follow these steps to configure WAN Edge cloud certificate authorization:

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Trust and Privacy** > **Certificates Settings** > **WAN Edge Cloud Certificate Authorization**
Choose from:

- Cisco PKI is the default option. To continue using Cisco PKI, follow these steps.
  a. Select **Sync Root Certificate** to migrate the Cisco IOS XE Catalyst SD-Routing devices in Cisco SD-WAN Manager to Cisco PKI.
  b. Select the **validity period** from the drop-down list.
- Alternatively, if you prefer to use **Enterprise Certificate**, follow these steps.
  a. Click **Enterprise Certificate**.

b. Click **Edit Settings**, to modify the settings. For more details, refer, *Configure enterprise certificate settings*.

c. If you want to specify custom certificate properties, click **Set CSR Properties** and configure the below parameters.

Parameter	Description
Domain Name	Network domain name
Organization	Organization name
Organizational Unit	Organizational unit name
Secondary Organization Unit	Secondary organizational Unit name
City	City name
State	State name
2-Letter Country Code	Email address
(Optional) Subject Alternative Name (SAN) DNS Names	You can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com
(Optional) Subject Alternative Name (SAN) URIs	You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

Step 2 Click **Save**.

WAN Edge cloud certificate authorization is complete.

Configure Hardware WAN Edge Certificate Authorization

To configure Hardware WAN Edge Certificate Authorization, follow these steps.

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Trust and Privacy** > **Certificates Settings** > **Hardware WAN Edge Certificate Authorization**
Choose from:

- Cisco PKI (SUDI Certificate) is the default option.
- Alternatively, if you prefer to use **Enterprise Certificate**, follow these steps.

a. Click **Enterprise Certificate**.

b. Click **Edit Settings**, to modify the settings. For more details, refer, *Configure enterprise certificate settings*.

c. If you want to specify custom certificate properties, click **Set CSR Properties** and configure the below parameters.

Parameter	Description
Domain Name	Network domain name
Organization	Organization name

Parameter	Description
Organizational Unit	Organizational unit name
Secondary Organization Unit	Secondary organizational Unit name
City	City name
State	State name
2-Letter Country Code	Email address
(Optional) Subject Alternative Name (SAN) DNS Names	You can configure multiple host names to use the same SSL certificate. Example, cisco.com and cisco2.com
(Optional) Subject Alternative Name (SAN) URIs	You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example, cisco.com and support.cisco.com

Step 2 Click **Save**.

Hardware WAN Edge certificate authorization is complete.

Configure enterprise certificate settings

From Cisco SD-WAN Manager go to **Administration** > **Settings** > **Trust and Privacy** > **Certificates Settings** page click **Enterprise Certificate Settings** to configure settings according to your preference.

The three enrollment protocol types are

- 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.

Enroll enterprise certificate manually

To manually enroll an enterprise certificate by uploading a root certificate authority file.

Follow these steps to enroll an enterprise certificate manually.

Step 1 Choose **Select a file** to upload a root certificate authority file. The uploaded root certificate authority displays in the text.

Step 2 Click **Save**.

The root certificate authority file is uploaded and saved.

Enroll enterprise certificate using EST

To enroll an enterprise certificate using the Enrollment over Secure Transport (EST) protocol.

You can configure certificate settings using either a username and password or a client certificate, depending on the CA server configuration.

Follow these steps to enroll an enterprise certificate using EST.

Step 1 Configure the following parameters.

Parameter	Description
URL base	Enter the full EST URL seen on CA server for EST/SCEP certificate authorization server.
(Optional) Username	Username for EST CA server authentication. Enter the same details here as per the configurations on the CA server.
(Optional) Password	Password for EST CA server authentication. Enter the same details here as per the configurations on the CA server.
(Optional) CA Label	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	Root CA cert chain of EST CA server. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.
Generate EST Client CSR	Click **Generate EST Client CSR** and configure the parameters to generate a CSR to create a certificate.
(Optional) Upload signed certificate	Use the **Select a File** option to upload a signed certificate. The signed certificate is obtained by signing the EST client CSR manually by CA

Step 2 Click **Save.**

Enterprise certificate enrollment using EST is configured.

Enroll enterprise certificate using SCEP

To enroll an enterprise certificate using the Simple Certificate Enrollment Protocol (SCEP).

Configure the following parameters.

Parameter	Description
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	Used for SCEP CA server authentication. Enter the same details here as per the configurations on the CA server
(Optional) Root CA fingerprint	Root CA certificate fingerprint used for verification. Use the md5 fingerprint of root CA
Root CA certificate	Root CA cert chain of SCEP CA server. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here

Enterprise certificate enrollment using SCEP is configured.

Renew enterprise certificate

To renew Enterprise certificates, follow these steps.

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

Step 2 On the WAN Edge List page, click **Certificate Management**.

Step 3 On the WAN Edges Certificate Management dialogue box, click **Let's do it**.

Step 4 Choose the certificate renewal type, **Auto** or **Manual** and click **Next.** Auto mode is for Cisco PKI and Enterprise (EST/SCEP). Manual mode is used for Enterprise CA to generate CSR and upload signed Certificate. Auto mode is available when you select enterprise SCEP/EST, or for Cisco PKI if a smart account is configured.

Step 5 Select the device(s) for renewal and click **Next**. Note, Customization of RSA key is available. Either select 2k or 4k based on your preference.

Step 6 (Optional) If you renew the enterprise certificate manually, follow these steps in the Renew and download CSR tab,

a) Generate and download CSR files(s) of selected WAN edges.
b) Upload signed certificate file or drag or drop the file
c) Click **Next**

Step 7 Schedule the renewal process either now or for a later date. Click **Next**.

Step 8 In the Summary tab, review the details and click **Complete**.

Certificate Renewal is scheduled.

Troubleshoot certificate management on CA server

The following table provides troubleshooting information for certificate management on the CA server.

Table 1:

Error Information	Possible Root Cause	Action
Internal Server `https://<est-url>:443/.well-known/est/simpleenroll HTTP Status Code: 500 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>500 Internal Server Error</title> </head><body>`	The CA server responds with a 500 server error. High CPU or memory usage on the CA server.	Check the CA server logs for error details. Increase the resource limits on the CA server 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. High CPU, memory usage, or maximum enrollment requests per minute cause this.	Increase resource limits or enrollment rate on the CA server.
Un-Authorized Error `Failed to get CSR signed for <device-id>, Failure reason - Simple Enroll: https://<est-url>:443/.well-known/est/simpleenroll HTTP Status Code: 401`	This error occurs if • EST configured with wrong/missing password (Users must provide password after modifying SD-WAN manager settings if CA server requires it) • EST client certificate lacks TLS authorization support. • EST Alias is not properly configured. • SCEP is configured with wrong/missing challenge password. Users must provide challenge password after modifying SD-WAN manager settings if CA server requires it	Identify and fix.
EST configuration Failed or Timed out resulting in Loss on OMP connection with controller	Sync of root-CA certificate fails on controllers due to failed Netconf, permission errors, or device/controller issues.	Identify and fix device specific problems.