Automated Certificate Management

Feature history for automated certificate management

Table 1: 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

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

An automated certificate management on Cisco SD-WAN Manager:

- uses protocols such as EST and SCEP to automate certificate enrollment and renewal for WAN edge devices, and
- introduces enterprise certificate settings to unify certificate management across controller components, hardware WAN edges, and cloud WAN edges.

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

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

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.

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.
- 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

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

Procedure

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

Step 2 Choose **Certificate settings** .

a) Configure the control component certificate authorization settings:

Table 2: Control Component Certificate Authorization

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.
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

b) Configure the WAN edge cloud certificate authorization settings

Table 3: 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

Table 4: Hardware WAN Edge Certificate Authorization

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 5: 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.	

Field	Description
Enterprise root certificate	Choose **Select a file** to upload a root certificate authority file. The uploaded root certificate authority displays in the text box.
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.

Step 3 Click **Save** .

Troubleshoot certificate management on CA server

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

Error type	Error message	Pausible root cause	Troubleshooting steps
Internal server error	https://<ca-url>:443/.well-known/est/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-url>:443/.well-known/est/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.