Cisco SD-WAN Control Components Certificate Management

SD-WAN Control Components certificate management feature history

Table 1: Feature History

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

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.

Supported environments for the Control Components Certificate Management workflow

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

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

Prerequisites for the Control Components Certificate Management workflow

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

  Enter Smart Account and Virtual Account details in Cisco SD-WAN Manager (**Administration** > **Settings** > **Smart Account Credentials**).

- 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**.

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.

Before you begin

See .

Procedure

Step 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.

Step 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.