Webex Share Security

About certificates

Most Cisco devices support wireless connection using X.509 certificates in addition to a password. If your company uses certificates for wireless connection, then you deploy the certificates before activating the device.

You create and manage certificates from the device setup web page, which you access by entering the device's IP address into a browser. When the device registers with Control Hub, the setup page becomes the device web page. If you don't see the setup page, then do a factory restart and return the device to the factory state.

If you decide to use certificates after deployment, then do a factory reset and delete the device from Control Hub. Reactivate the device by generating a second activation code. But don't register the device with Control Hub until after you deploy the certificates.

Generate a Certificate

You generate the certificate before you activate your device. If you want to use EAP-TLS for Wi-Fi or for 802.1x, obtain a device certificate and then load the CA certificates to your device.

Before you begin

- Connect your device to your network.
- Obtain the device IP address.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address for your device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Select **Enroll Certificates**.

Step 4 Fill in the fields:

- Common Name—The room name or name that identifies the device.
- Organizational Unit Name—The department name making the certificate request. For example Finance or IT.
- Organizational Name—The full legal company name making the certificate request. Include any suffixes such as Ltd. or Corp.
- Location—The city or town where the company is located.
- State—The full state name where the company is located. Do not abbreviate.
- Country—The two-letter ISO code for the country where your organization is located. For example, US, GB, FR.
- Key size: 2048 or 4096
- Key size: 2048 or 4096
- Certificate Usage—Check one or more of the following
  - **EAP/TLS** for wireless connections
  - **802.1x** for wired connections
- Extended Key Usage options—Select both of the following extensions:
  - **serverAuth** for server authentication
  - **clientAuth** for client authentication

Step 5 Click **Generate**.

What to do next

Get the certificate signed.

Download and sign the certificate

After you generate your certificate, download the certificate signing request (CSR) so it can be completed.

Before you begin

You have generated an unsigned certificate request for this device.

Obtain the device IP address for your device.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address of the device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Select **Manage Certificates**.

Step 4 Click **Download**.

The certificate downloads to your computer.

Step 5 Get the downloaded certificate signing request (CSR) signed. Follow your organization's customary procedure.

What to do next

After you get the CSR signed, upload the signed certificate.

Upload the certificate

Upload a certificate to your server. The appropriate authority must sign it first.

Before you begin

Obtain the device IP address.

Verify that the certificate is in Privacy-Enhanced Mail(PEM) format.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address of the device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Select **Manage Certificates**.

Step 4 Under Upload signed certificate, click **Upload**. Navigate to the certificate's location.

If you upload the wrong certificate, find the correct one and upload it.

Add a certificate authority or root certificate

Before you begin

You have a certificate authority (CA) or root certificate to upload to be used with wifi or 802.1x authentication.

Obtain the device IP address.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address of the device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Click **Add CA/root Certificate**.

Step 4 Choose at least one of the following:

802.1x

EAP/TLS

Digital Signage

Step 5 Click **Upload certificate**.

Configure Wi-Fi settings to support certificates

After you upload the signed certificates, configure the Wi-Fi settings and select your certificate.

Before you begin

Obtain the device IP address.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address of the device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Go to **Network** > **Wi-Fi**.

Step 4 Choose an SSID.

Step 5 Click the first drop-down list box to show the supported protocols.

Step 6 Choose **EAP-TLS**.

Step 7 In Choose Client Certificate, choose a certificate.

Step 8 In Choose CA Certificate, choose a certificate.

Step 9 (Optional) Fill in a username.

Step 10 Click **Join**.

Enroll an Ethernet 802.1X certificate

You need an Ethernet 802.1x certificate for devices that use Wi-Fi.

Obtain the device IP address.

Before you begin

Generate a certificate with the 802.1x protocol and get it signed.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address of the device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Select **Ethernet 802.1X Certificate**.

Step 4 Select the certificate from the drop-down list.

Step 5 Click **Select**.

View available certificates

After you upload a certificate, you can view the certificate information. This is useful when troubleshooting an issue.

Before you begin

Obtain the device IP address.

Procedure

Step 1 Open a web browser and enter the following URL, where *IP address* is the IP address of the device:

`http://`*IP address*

Step 2 Navigate **Setup** > **Add certificate**.

Step 3 Select **Enroll Certificates**.

Step 4 Click **Info** to view information about a certificate.

Each certificate shows:

- Common Name—The fully qualified domain name
- Cert Type—Values are CSR certificate, Local, CA/Root
- Cert Usage—Lists the protocols that a certificate supports (802.1x, EAP/TLS)

Step 5 (Optional) If needed, click **Delete** to delete a certificate.