Enable Third-Party CA Signed Certificate

This section explains the following:

Enable Third-Party CA Signed Certificate

You can import your company signed certificate for the secured data transmission. SSL must be enabled on the browser to use this certificate.

Install CA signed certificate

Steps to install CA signed certificate for secure data transmission:

Before you begin

The following factors will be validated to protect information assets for strong security, easy administration, and hands-on control of certificate management.

For Cisco Prime Collaboration Release 12.1 SP3 and later

The CA Signed Certificate must meet the following list of requirements. It must

- Contain “primecollab” alias.
- Allow importing with the right password.
- Stay valid for more than 30 years.
- Have the valid validity period. The validity must not
  - Expire

    Ex: If Current Date is 20/9/2019, Validity period (20/8/1970-20/8/2000) is invalid.
  - Have a future date

    Ex: If Current Date is 20/9/2019, Validity period (20/12/2020-20/12/2025) is invalid.
  - A “Sample valid” validity period

    Ex: If Current Date is 20/9/2019, Validity period (20/9/2019-20/9/2025) is valid.

- CN (common name) or SAN (Subject Alternative Name) specified in the certificate must match with FQDN (Fully Qualified Domain Name) of the PCA server.
  - If FQDN of the PCA server does not match with the CN, it is matched with the list of SANs.
  - Users must either generate CSR (Certificate Signing Request) with CN as FQDN or include FQDN in the list of SANs. Ex: pcatest.cisco.com (FQDN).
- Signature algorithm must match with the Signature Algorithm Identifier present in the TBSCertificate sequence.
- Not have any duplicate extensions.
- Not have any un-supported critical extensions.
  - Check applies only on extensions marked as critical.
  - Extensions supported are BC or BasicConstraints, KU or KeyUsage, EKU or ExtendedkeyUsage, SAN or SubjectAlternativeName, IAN or IssuerAlternativeName, SIA or SubjectInfoAccess, AIA or AuthorityInfoAccess.
- Have a valid critical KeyUsage (KU)
  - Check applies if KU extension is marked as critical.
  - Valid KUs are keyCertSign, cRLSign, digitalSignature.
- Have a valid critical ExtendedKeyUsage (EKU).
  - Check applies if EKU extension is marked as critical.
  - Valid EKUs are serverAuth , clientAuth, OCSPSigning.

If any of the above requirements are not satisfied, the certificate is rejected and user is alerted with an appropriate error message.

For Cisco Prime Collaboration Release 11.5 and later

- The Root Certificate is part of the Signed Certificate.
- SSL is enabled on the browser to use CA signed certificate.

Step 1 Choose **System Administration** > **Certificate Management** > **Cisco Prime Collaboration Certificate Management**.

Step 2 Browse through the CA signed Certificate (in PKCS12 format) from your local system.

Step 3 (Optional) Enter and verify the certificates password of PKCS#12 file, if you have configured the password while generating the certificate, otherwise it can be left empty.

Step 4 Click **Import**.

A warning message indicating that "The services will be restarted" appears.

Step 5 Click **Continue** on receiving the warning message.
The certificates are successfully imported on the server.

Note You must manually restart the Cisco Prime Collaboration Assurance server after you import the certificates.

For Cisco Prime Collaboration Release 12.1 SP3 and later

To restart Cisco Prime Collaboration Assurance server, login as *root* and execute the following commands:

1. Stop the processes:

```
root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh stop
```

2. Check the status of the processes - Verify whether the processes have stopped:

```
root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh status
```

3. Restart the processes:

```
root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh start
```

After the service restart, the login page is displayed. The security warning page (where you make the selection for the login page to appear) is no longer displayed.

Note Before you launch the Cisco Prime Collaboration Assurance server, we recommend that you import the primary and secondary intermediate certificates to the browser. This ensures that you do not get a warning about your connection not being private, when you launch the server for the first time after the CA signed certificate installation.

You can import PKCS12 certificate with any alias name.

You should use the certificates in PKCS#12 (.pfx or .p12) format as PEM/DER (.pem, .cer, .der, .key, and so on) formats are not supported.

For Cisco Prime Collaboration Release 11.6 and later

Note Make sure you import a PKCS12 (.pfx or .p12) format signed certificate.

The certificate must contain **primecollab** alias.

The Key password for **primecollab** alias must be same as the certificate password.

For Cisco Prime Collaboration Release 12.1 and later

If a PKCS7 or PKCS12 certificate is applied to 11.x and the Cisco Prime Collaboration Assurance is migrated to version 12.1, the certificate will not be restored. You need to regenerate the certificate for the Cisco Prime Collaboration Assurance 12.1.

Note From Cisco Prime Collaboration Assurance 11.6 onwards, only PKCS12 certificate is supported.

To import the primary/intermediate/secondary certificates to the browser, see the following table:

Browser	Action
Internet Explorer	Choose **Tools** > **Internet Options** > **Content** > **Certificates** > **Trusted root certification authorities** > **Import**
Mozilla Firefox	Choose **Tools** > **Options** > **Advanced** > **Certificates** > **View certificates** > **Import**

Browser	Action
Chrome	Choose **Settings** > **Advanced settings** > **HTTP/SSL Manage certificates** > **Trusted root certification authorities** > **Import**