



Certificate Monitoring and Revocation

- [Certificate Monitoring Overview, on page 1](#)
- [Certificate Monitoring Task Flow, on page 2](#)

Certificate Monitoring Overview

Administrators must be able to keep track of certificates. Part of this is knowing which certificates need to be renewed and when. Cisco Unified Communications Manager contains automated systems that help administrators to know which certificates are approaching renewal and when. You can configure the system to do the following:

- Monitor certificate statuses on an ongoing basis and email you when a certificate is approaching expiration.
- Use the Online Certificate Status Protocol (OCSP) to check certificate status regularly and revoke certificates as they expire.

Certificate Revocation through Online Certificate Status Protocol

Unified Communications Manager provisions the OCSP for monitoring certificate revocation. System checks for the certificate status to confirm validity at scheduled intervals and every time there is, a certificate uploaded.

The Online Certificate Status Protocol (OCSP) helps administrators manage their system's certificate requirements. When OCSP is configured, it provides a simple, secure, and automated method to check certificate validity and revoke expired certificates in real-time.

For FIPS deployments with Common Criteria mode enabled, OCSP also helps your system comply with Common Criteria requirements.

Validation Checks

Unified Communications Manager checks the certificate status and confirms validity.

The certificates are validated as follows:

- Unified Communications Manager uses the Delegated Trust Model (DTM) and checks the Root CA or Intermediate CA for the OCSP signing attribute. The Root CA or the Intermediate CA must sign the OCSP Certificate to check the status. If the delegated trust model fails, Unified Communications Manager falls back to the Trust Responder Model (TRP) and uses a designated OCSP response signing certificate from an OCSP server to validate certificates.



Note OCSP Responder must be running to check the revocation status of the certificates.

- Enable OCSP option in the **Certificate Revocation** window to provide the most secure means of checking certificate revocation in real-time. Choose from options to use the OCSP URI from a certificate or from the configured OCSP URI. For more information on manual OCSP configuration, see [Configure Certificate Revocation via OCSP](#).



Note In case of leaf certificates, TLS clients like syslog, FileBeat, SIP, ILS, LBM, and so on send OCSP requests to the OCSP responder and receives the certificate revocation response in real-time from the OCSP responder.

One of the following status is returned for the certificate once the validations are performed and the Common Criteria mode is ON.

- **Good** --The **good** state indicates a positive response to the status inquiry. At a minimum, this positive response indicates that the certificate is not revoked, but does not necessarily mean that the certificate was ever issued or that the time at which the response was produced is within the certificate's validity interval. Response extensions may be used to convey additional information on assertions made by the responder regarding the status of the certificate such as positive statement about issuance, validity, etc.
- **Revoked** --The **revoked** state indicates that the certificate has been revoked (either permanently or temporarily (on hold)).
- **Unknown** -- The **unknown** state indicates that the OCSP responder doesn't know about the certificate being requested.



Note In Common Criteria mode, the connection fails in both **Revoked** as well as **Unknown** case whereas the connection would succeed in **Unknown** response case when Common Criteria is not enabled.

Certificate Monitoring Task Flow

Complete these tasks to configure the system to monitor certificate status and expiration automatically.

- Email you when certificates are approaching expiration.
- Revoke expired certificates.

Procedure

	Command or Action	Purpose
Step 1	Configure Certificate Monitor Notifications, on page 3	Configure automatic certificate monitoring. The system periodically checks certificate statuses

	Command or Action	Purpose
		and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 4	Configure the OCSP so that the system revokes expired certificates automatically.

Configure Certificate Monitor Notifications

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.



Note The **Cisco Certificate Expiry Monitor** network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing **Tools > Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

- Step 1** Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).
- Step 2** Choose **Security > Certificate Monitor**.
- Step 3** In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.
- Step 4** In the **Notification Frequency** fields, enter the frequency of notifications.
- Step 5** Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations..
- Step 6** Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.
- Step 7** In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.
- Step 8** Click **Save**.

Note The certificate monitor service runs once every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

What to do next

Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, see [Configure Certificate Revocation via OCSP, on page 4](#)

Configure Certificate Revocation via OCSP

Enable the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically.

Before you begin

Make sure that your system has the certificates that are required for OCSP checks. You can use Root or Intermediate CA certificates that are configured with the OCSP response attribute or you can use a designated OCSP signing certificate that has been uploaded to the tomcat-trust.

Procedure

- Step 1** Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).
- Step 2** Choose **Security > Certificate Revocation**.
- Step 3** Check the **Enable OCSP** check box, and perform one of the following tasks:
- If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.
 - If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.
- Step 4** Check the **Enable Revocation Check** check box.
- Step 5** Complete the **Check Every** field with the interval period for revocation checks.
- Step 6** Click **Save**.
- Step 7** Optional. If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long-lived connections:
- a) From Cisco Unified CM Administration, choose **System > Enterprise Parameters**.
 - b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.
 - c) Configure a value for the **Validity Check Frequency** parameter.
- Note** The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.
- d) Click **Save**.
-