Certificate Revocation/Expiry Status Verification

This chapter provides a brief overview of how to check the status of the certificates generated for sessions in Unified Communications Manager Administration. The certificate service periodically checks for long lived sessions between Unified Communications Manager and other services. Long lived sessions have duration of six hours or more. The check is performed for the following long lived sessions:

- CTI Connections with JTAPI /TAPI applications.
- LDAP Connection between Unified Communications Manager and SunOne servers.
- IPSec Connections

It also describes how to configure the enterprise parameter for verifying certificate revocation and expiry.

The enterprise parameter **Certificate Revocation and Expiry** allows you to control the certificate validation checks. The revocation and expiry check parameter is enabled on the **Enterprise Parameter** page of Unified Communications Manager. The certificate expiry for the long lived sessions is not verified, when the enterprise parameter value is disabled.

The certificate revocation service is active for LDAP and IPSec connections, when the **Enable Revocation** is selected on the Operating System Administration of Unified Communications Manager and revocation and expiry check parameter is set to enabled. The periodicity of the check for IPSec connections are based on the **Check Every** value. The revocation check for the certificate is not performed, if the **Enable Revocation** check box is unchecked.

Note The GeneralizedTime values for X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile must be expressed in Greenwich Mean Time (GMT) and must include seconds (i.e., times are **YYYYMMDDHHMMSSZ**), even when the number is zero. GeneralizedTime values must not include the fractional seconds. If the peer entity offers a certificate which violates this rule or a certificate is loaded in the trust stores from the peer entities, then it could possibly fail the certificate verification process.

Certificate Revocation/Expiry Status Verification

This chapter provides a brief overview of how to check the status of the certificates generated for sessions in Unified Communications Manager Administration. The certificate service periodically checks for long lived sessions between Unified Communications Manager and other services. Long lived sessions have duration of six hours or more. The check is performed for the following long lived sessions:

- CTI Connections with JTAPI /TAPI applications.
- LDAP Connection between Unified Communications Manager and SunOne servers.
- IPSec Connections

It also describes how to configure the enterprise parameter for verifying certificate revocation and expiry.

The enterprise parameter **Certificate Revocation and Expiry** allows you to control the certificate validation checks. The revocation and expiry check parameter is enabled on the **Enterprise Parameter** page of Unified Communications Manager. The certificate expiry for the long lived sessions is not verified, when the enterprise parameter value is disabled.

The certificate revocation service is active for LDAP and IPSec connections, when the **Enable Revocation** is selected on the Operating System Administration of Unified Communications Manager and revocation and expiry check parameter is set to enabled. The periodicity of the check for IPSec connections are based on the **Check Every** value. The revocation check for the certificate is not performed, if the **Enable Revocation** check box is unchecked.

Note The GeneralizedTime values for X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile must be expressed in Greenwich Mean Time (GMT) and must include seconds (i.e., times are **YYYYMMDDHHMMSSZ**), even when the number is zero. GeneralizedTime values must not include the fractional seconds. If the peer entity offers a certificate which violates this rule or a certificate is loaded in the trust stores from the peer entities, then it could possibly fail the certificate verification process.

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 and emails you when a certificate is approaching expiration.

	Command or Action	Purpose
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, seeConfigure 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**.

Support for Delegated Trust Model in OCSP Response

Online Certificate Status Protocol (OCSP) allows a device to obtain real-time information about the status of a given certificate. Examples of certificate status are Good, Revoked, and Unknown.

Unified Communications Manager uses OCSP to validate third-party certificates that are uploaded into the Unified Communications Manager trust store. Unified Communications Manager requires an OCSP Responder URL to connect to the OCSP responder server over HTTP. It sends an HTTP request to the responder to validate a certificate.

Unified Communications Manager currently supports the Trusted Responder Model of OCSP, where the OCSP response is signed by a self-signed certificate of the OCSP server. This self-signed certificate is uploaded to the trust store before initiating an OCSP request. This certificate is used to verify the signature on the OCSP response.

Unified Communications Manager 11.0 and later support the Delegated Trust Model (DTM) of the OCSP responder, where the OCSP responses are no longer approved by the self-signed certificate but are issued by a Certificate Authority (Root CA or Subordinate CA). The CA certificate validates the OCSP responder certificates. The CA certificate that issued the OCSP responder certificate in Unified Communications Manager trust store is required, instead of OCSP response signing certificate. When you receive an OCSP response, the CA's certificate is used to validate the signature in the response.

Note In case of a DTM execution failure, the OCSP response is verified using the self-signed certificate.