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.

Verify Certificate Status

The following procedure provides the tasks that you perform to enable or disable the certificate validity check.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**

The Enterprise Parameters Configuration window displays.

Step 2 Under **Certificate Revocation and Expiry** section,

a) From the **Certificate Validity Check** drop-down list box, select Enabled to enable the validity check.
b) Enter the **Validity Check Frequency (hours)** value.

The default value is 24 hours. The minimum value is 6 hours and the maximum value is 576 hours.

Step 3 Click Save.

Step 4 Click Apply Config.

The Apply Configuration Information dialog displays.

Step 5 Click Ok.

The timers for DIRSYNC and CTI are restarted.

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.