Certificate Revocation Overview

This section allows you to understand certificate revocation. Cisco UCM provisions the Online Certificate Status Protocol (OCSP) for monitoring certificate revocation. Every time there's a certificate uploaded and at scheduled timelines, system checks for its status to confirm validity.

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

- Certificate Revocation Configuration, on page 1

Certificate Revocation Configuration

Validation Checks Unified Communications Manager checks the status of the certificate and confirms validity.

The certificate validation procedure is 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, falls back to the Trust Responder Model (TRP). Unified Communications Manager then 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.

Configure OCSP so that the system revokes expired certificates automatically. Enable OCSP option in the Certificate Revocation window to provide a secure means of checking certificate revocation in real time. Choose from options to use the OCSP URI from certificate or from the configured OCSP URI.

Note TLS clients like syslog, FileBeat, SIP, ILS, LBM, and so on, receive the revocation response in real time from OCSP.

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

Procedure

Step 1 From the Cisco Unified OS Administration, choose **Security** > **Certificate Revocation.**

Step 2 Check the **Enable OCSP** check box.

Step 3 Click the **Use OCSP URI from Certificate** option if the certificate is configured with an OCSP responder URI.

OR

Step 4 Click **Use Configured OCSP URI** option if you want to specify an OCSP responder for OCSP checks.

Step 5 Enter the **OCSP Configured URI** of the responder.

Step 6 Check the **Enable Revocation Check** check box to enable a revocation check.

Step 7 Enter a **frequency** to check for revocation status and click the **time interval** from Hours or Days.

Step 8 Click **Save**.

Note A popup alerts you to restart a list of Cisco Services and enable realtime OCSP. The popup appears only when you check the **Enable OCSP** check box or save the subsequent changes.

The OCSP Responder return one of the following statuses based on the validations and when the Common Criteria mode is ON.

- **Good—** indicates that the OCSP responder sends a positive response to the status inquiry. The certificate isn't revoked but doesn't mean that the certificate was ever issued or the response time is within the validity interval of the certificate. Response extensions convey more claims made by the responder on the certificate status such as issuance, validity, and so on.
- **Revoked—** indicates that the certificate is in revoked (on hold) status either permanently or temporarily.
- **Unknown—** indicates that the OCSP responder doesn't know about the requested certificate.

Warning When you enable Common Criteria mode, the connection fails in **Revoked** and **Unknown** cases. When you disable Common Criteria mode, the connection succeeds in **Unknown** case.

Step 9 (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 uninterrupted connections:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
b) Navigate to **Certificate Revocation and Expiry** pane.
c) Set the **Certificate Validity Check** parameter to **Enabled**.
d) Enter a value for the **Validity Check Frequency** parameter.

Note The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** page takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

e) Click **Save**.