Manage Certificates

Certificates Overview

Your system uses self-signed- and third-party-signed certificates. Certificates are used between devices in your system to securely authenticate devices, encrypt data, and hash the data to ensure its integrity from source to destination. Certificates allow for secure transfer of bandwidth, communication, and operations.

The most important part of certificates is that you know and define how your data is encrypted and shared with entities such as the intended website, phone, or FTP server.

When your system trusts a certificate, this means that there is a preinstalled certificate on your system which states it is fully confident that it shares information with the correct destination. Otherwise, it terminates the communication between these points.

In order to trust a certificate, trust must already be established with a third-party certificate authority (CA).

Your devices must know that they can trust both the CA and intermediate certificates first, before they can trust the server certificate presented by the exchange of messages called the secure sockets layer (SSL) handshake.

Note EC-based certificates for Tomcat are supported. This new certificate is called tomcat-ECDSA. For further information, see the Enhanced TLS Encryption on IM and Presence Service section of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

EC Ciphers on the Tomcat interface are disabled by default. You can enable them using the **HTTPS Ciphers** enterprise parameter on Cisco Unified Communications Manager or on IM and Presence Service. If you change this parameter the Cisco Tomcat service must be restarted on all nodes.

For further information on EC-based certificates see, ECDSA Support for Common Criteria for Certified Solutions in the Release Notes for Cisco Unified Communications Manager and IM and Presence Service.

Third-Party Signed Certificate or Certificate Chain

Upload the certificate authority root certificate of the certificate authority that signed an application certificate. If a subordinate certificate authority signs an application certificate, you must upload the certificate authority root certificate of the subordinate certificate authority. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates.

You can upload certificate authority root certificates and application certificates by using the same **Upload Certificate** dialog box. When you upload a certificate authority root certificate or certificate chain that contains only certificate authority certificates, choose the certificate name with the format certificate type-trust. When you upload an application certificate or certificate chain that contains an application certificate and certificate authority certificates, choose the certificate name that includes only the certificate type.

For example, choose **tomcat-trust** when you upload a Tomcat certificate authority certificate or certificate authority certificate chain; choose **tomcat** or **tomcat-ECDSA** when you upload a Tomcat application certificate or certificate chain that contains an application certificate and certificate authority certificates.

When you upload a CAPF certificate authority root certificate, it is copied to the CallManager-trust store, so you do not need to upload the certificate authority root certificate for CallManager separately.

Note Successful upload of third-party certificate authority signed certificate deletes a recently generated CSR that was used to obtain a signed certificate and overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Note The system automatically replicates tomcat-trust, CallManager-trust and Phone-SAST-trust certificates to each node in the cluster.

Note You can upload a directory trust certificate to tomcat-trust, which is required for the DirSync service to work in secure mode.

Third-Party Certificate Authority Certificates

To use an application certificate that a third-party certificate authority issues, you must obtain both the signed application certificate and the certificate authority root certificate from the certificate authority or PKCS#7 certificate chain (distinguished encoding rules [DER]), which contains both the application certificate and certificate authority certificates. Retrieve information about obtaining these certificates from your certificate authority. The process varies among certificate authorities. The signature algorithm must use RSA encryption.

Cisco Unified Communications Operating System generates CSRs in privacy enhanced mail (PEM) encoding format. The system accepts certificates in DER and PEM encoding formats and PKCS#7 Certificate chain in PEM format. For all certificate types except certificate authority proxy function (CAPF), you must obtain and upload a certificate authority root certificate and an application certificate on each node.

For CAPF, obtain and upload a certificate authority root certificate and an application certificate only on the first node. CAPF and Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the certificate authority. If your certificate authority does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, as follows:

- The CAPF CSR uses the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Key Usage:
Digital Signature, Certificate Sign
```

- The CSRs for Tomcat and Tomcat-ECDSA, use the following extensions:

Note Tomcat or Tomcat-ECDSA does not require the key agreement or IPsec end system key usage.

```
X509v3 Extended Key Usage:
 TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System

 X509v3 Key Usage:
 Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for IPsec use the following extensions:

```
 X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for Unified Communications Manager use the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for the IM and Presence Service cup and cup-xmpp certificates use the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement,
```

Note You can generate a CSR for your certificates and have them signed by a third party certificate authority with a SHA256 signature. You can then upload this signed certificate back to Unified Communications Manager, allowing Tomcat and other certificates to support SHA256.

Certificate Signing Request Key Usage Extensions

The following tables display key usage extensions for Certificate Signing Requests (CSRs) for both Unified Communications Manager and the IM and Presence Service CA certificates.

Table 1: Cisco Unified Communications Manager CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF (publisher only)	N	Y			Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	N	Y	Y		Y	Y	Y		

Table 2: IM and Presence Service CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

Note Ensure that 'Data Encipherment' bit is not changed or removed as part of the CA-signing certificate process.

Show Certificates

Use the filter option on the Certificate List page, to sort and view the list of certificates, based on their common name, expiry date, key type, and usage. The filter option thus allows you to sort, view, and manage your data effectively.

From Unified Communications Manager Release 14, you can choose the usage option to sort and view the list of identity or trust certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The Certificate List page appears.

Step 2 From the **Find Certificate List where** drop-down list, choose the required filter option, enter the search item in the **Find** field, and click the **Find** button.

For example, to view only identity certificates, choose **Usage** from the **Find Certificate List where** drop-down list, enter Identity in the **Find** field, and click the **Find** button.

Download Certificates

Use the download certificates task to have a copy of your certificate or upload the certificate when you submit a CSR request.

Procedure

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

Step 2 Specify search criteria and then click **Find**.

Step 3 Choose the required file name and Click **Download**.

Install Intermediate Certificates

To install an intermediate certificate, you must install a root certificate first and then upload the signed certificate. This step is required only if the certificate authority provides a signed certificate with multiple certificates in the certificate chain.

Procedure

Step 1 From Cisco Unified OS Administration, click **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate / Certificate Chain**.

Step 3 Choose the appropriate trust store from the **Certificate Purpose** drop-down list to install the root certificate.

Step 4 Enter the description for the certificate purpose selected.

Step 5 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse** and navigate to the file; then click **Open**.

Step 6 Click **Upload**.

Step 7 Access the Cisco Unified Intelligence Center URL using the FQDN after you install the customer certificate. If you access the Cisco Unified Intelligence Center using an IP address, you will see the message “Click here to continue”, even after you successfully install the custom certificate.

Note
- TFTP service should be restarted when a Tomcat certificate is uploaded. Else, the TFTP continues to offer the old cached self-signed tomcat certificate.
- Uploading certificates from phone edge trust should be done from publisher.

Delete a Trust Certificate

A trusted certificate is the only type of certificate that you can delete. You cannot delete a self-signed certificate that is generated by your system.

Caution Deleting a certificate can affect your system operations. It can also break a certificate chain if the certificate is part of an existing chain. Verify this relationship from the username and subject name of the relevant certificates in the **Certificate List** window. You cannot undo this action.

Procedure

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

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note
- If you delete the “CAPF-trust”, “tomcat-trust”, “CallManager-trust”, or “Phone-SAST-trust” certificate type, the certificate is deleted across all servers in the cluster.
- Deletion of certificates from phone edge trust should be done from publisher.
- If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across the cluster.

Regenerate a Certificate

We recommend you to regenerate certificates before they expire. You will receive warnings in RTMT (Syslog Viewer) and an email notification when the certificates are about to expire.

However, you can also regenerate an expired certificate. Perform this task after business hours, because you must restart phones and reboot services. You can regenerate only a certificate that is listed as type “cert” in Cisco Unified OS Administration

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Procedure

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

Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the **Certificate List** window.

Click **Regenerate** button in certificate details page, a self-signed certificate with the same key length is regenerated.

Note When regenerating a certificate, the **Certificate Description** field is not updated until you close the **Regeneration** window and open the newly generated certificate.

Click **Generate Self-Signed Certificate** to regenerate a self-signed certificate with a new key length of 3072 or 4096.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate. See Certificate Names and Descriptions, on page 8 for more information.

Step 5 Update the CTL file (if configured) after you regenerate the CAPF, ITLRecovery Certificates or CallManager Certificates.

Note After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register.

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 3: Certificate Names and Descriptions

Name	Description	Services to be Restarted
tomcat tomcat-ECDSA	This certificate is used by WebServices, Cisco DRF Services, and Cisco CallManager Services when SIP Oauth mode is enabled.	Cisco Tomcat Services, Cisco CallManager Service.
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	Cisco Call Manager Service and other relevant services including Cisco CTI Manager - update CTL file if the server is in secure mode. CallManager-ECDSA - Cisco CallManager Service.
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode)	N/A
TVS	This is used by Trust verification service, which acts as a secondary trust verification mechanism for the phones in case the server certificate changes.	N/A

Important This note is applicable for Release 14SU2 only.

For Release 14SU2, Cisco DRF services needs restart post tomcat-ECDSA certificate regeneration or upload. Restart is not needed post tomcat RSA certificate operations.

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the **AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.

b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.

b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Note Restart the Cisco CallManager Service on all nodes in the cluster after the keys are reassigned.

Upload Certificate or Certificate Chain

Upload any new certificates or certificate chains that you want your system to trust.

Procedure

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

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse**, navigate to the file, and then click **Open**.

Step 5 To upload the file to the server, click **Upload File**.

Note Restart the affected service after uploading the certificate. When the server comes back up you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

Manage Third-Party Certificate Authority Certificates

This task flow provides an overview of the third-party certificate process, with references to each step in the sequence. Your system supports certificates that a third-party certificate authority issues with a PKCS # 10 certificate signing request (CSR).

Procedure

	Command or Action	Purpose
Step 1	Generate a Certificate Signing Request, on page 11	Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.
Step 2	Download a Certificate Signing Request, on page 11	Download the CSR after you generate it and have it ready to submit to your certificate authority.
Step 3	See your certificate authority documentation.	Obtain application certificates from your certificate authority.
Step 4	See your certificate authority documentation.	Obtain a root certificate from your certificate authority.
Step 5	Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store , on page 12	Add the root certificate to the trust store. Perform this step when using a certificate authority-signed CAPF certificate.
Step 6	Upload Certificate or Certificate Chain, on page 9	Upload the certificate authority root certificate to the node.
Step 7	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file.	See the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

	Command or Action	Purpose
		Rerun the CTL client (if configured) after you upload the third-party signed CAPF or CallManager certificate.
Step 8	Restart a Service, on page 12	Restart the services that are affected by the new certificate. For all certificate types, restart the corresponding service (for example, restart the Cisco Tomcat service if you updated the Tomcat or Tomcat-ECDSA certificate).

Generate a Certificate Signing Request

Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.

Note If you generate a new CSR, you overwrite any existing CSRs.

Procedure

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

Step 2 Click **Generate CSR**.

Step 3 Configure fields on the **Generate Certificate Signing Request** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Generate**.

Download a Certificate Signing Request

Download the CSR after you generate it and have it ready to submit to your certificate authority.

Procedure

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

Step 2 Click **Download CSR**.

Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Click **Download CSR**.

Step 5 (Optional) If prompted, click **Save**.

Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store

Add the root certificate to the Unified Communications Manager trust store when using a Certificate Authority-Signed CAPF Certificate.

Procedure

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

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 In the **Upload Certificate/Certificate Chain** popup window, choose **CallManager-trust** from the **Certificate Purpose** drop-down list and browse to the certificate authority-signed CAPF root certificate.

Step 4 Click **Upload** after the certificate appears in the **Upload File** field.

Restart a Service

Use this procedure if your system requires that you restart any feature or network services on a particular node in your cluster.

Procedure

Step 1 Depending on the service type that you want to restart, perform one of the following tasks:

- Choose **Tools** > **Control Center - Feature Services**.
- Choose **Tools** > **Control Center - Network Services**.

Step 2 Choose your system node from the **Server** drop-down list, and then click **Go**.

Step 3 Click the radio button next to the service that you want to restart, and then click **Restart**.

Step 4 After you see the message that indicates that the restart will take some time, click **OK**.

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 permanantly 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 14	Configure automatic certificate monitoring. The system periodically checks certificate statuses and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 15	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 15

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**.

Troubleshoot Certificate Errors

Before you begin

If you encounter an error when you attempt to access Unified Communications Manager services from an IM and Presence Service node or IM and Presence Service functionality from a Unified Communications Manager node, the source of the issue is the tomcat-trust certificate. The error message `Connection to the Server cannot be established (unable to connect to Remote Node)` appears on the following Serviceability interface windows:

- **Service Activation**
- **Control Center - Feature Services**
- **Control Center - Network Services**

Use this procedure to help you resolve the certificate error. Start with the first step and proceed, if necessary. Sometime, you may only have to complete the first step to resolve the error; in other cases, you have to complete all the steps.

Procedure

Step 1 From Cisco Unified OS Administration, verify that the required tomcat-trust certificates are present: **Security** > **Certificate Management**.

If the required certificates are not present, wait 30 minutes before checking again.

Step 2 Choose a certificate to view its information. Verify that the content matches with the corresponding certificate on the remote node.

Step 3 From the CLI, restart the Cisco Intercluster Sync Agent service: **utils service restart Cisco Intercluster Sync Agent**.

Step 4 After the Cisco Intercluster Sync Agent service restarts, restart the Cisco Tomcat service: **utils service restart Cisco Tomcat**.

Step 5 Wait 30 minutes. If the previous steps do not address the certificate error and a tomcat-trust certificate is present, delete the certificate. After you delete the certificate, you must manually exchange it by downloading the Tomcat and Tomcat-ECDSA certificate for each node and uploading it to its peers as a tomcat-trust certificate.

Step 6 After the certificate exchange is complete, restart Cisco Tomcat on each affected server: **utils service restart Cisco Tomcat**.