Certificate Overview

Certificates Overview

A certificate is a file that contains the certificate holder name, public key and digital signature of the certificate authority that is issuing the certificate. A certificate proves the identity of the owner of the certificate.

Unified Communications Manager uses certificates that use the public-key infrastructure (PKI) in order to validate server and client identity and to enable encryption. When another system (for example, a phone or media server) tries to connect to Unified Communications Manager, it presents its certificate to Unified Communications Manager in order to verify its identity. Unified Communications Manager will not trust the other system, and will deny access, unless it has a matching certificate in the appropriate trust store.

Unified Communications Manager uses two broad classes of certificates:

- Self-signed Certificates—By default, Unified Communications Manager uses self-signed certificates. These are certificates where Unified Communications Manager itself signs the certificate in order to confirm the identity of the server or client. Unified Communications Manager can issue self-signed certificates for itself, or for LSC certificates on behalf of phones via the Certificate Authority Proxy Function.

- CA-signed certificates—You can also configure Unified Communications Manager to use certificates that are signed by a third-party certificate authority (CA). You must complete a Certificate Signing Request (CSR) to have the CA sign a certificate on behalf of Unified Communications. The CA receives the request and issues CA-signed certificates. To use CA-signed certificates, you must first install the CA root certificate chain on Unified Communications Manager.

Note Typically, self-signed certificates are accepted for internal connections that do not cross a company firewall. However, for WAN connections, or for connections that use the public internet, you should use CA-signed certificates.

Note Generalized Time values for X.509 PKI certificates must be expressed in Greenwich Mean Time (GMT) and must include seconds (**YYYYMMDDHHMMSSZ**). Fractional seconds are not allowed. Certificates that violate this rule, whether offered from a peer entity, or loaded in the trust store, may fail the certificate verification process.

CTL File

The Cisco Certificate Trust List is a file that is created when you enable mixed mode by the Cisco CTL Client or by running one of the utils ctl CLI commands (for example, utils ctl update CTLFile). When mixed mode is enabled, the CTL file gets installed on Cisco IP Phones via the TFTP server. The CTL file contains a list of certificates for phones to trust, including the Certificate Authority Proxy Function system certificate and other certificates.

For details on how to configure the CTL File, see the CTL Client Setup chapter.

TLS

Transport Line Signaling (TLS) uses CA-signed certificates. When TLS is configured, the other system presents its certificate to Unified Communications Manager as part of the initial connection setup. If Unified Communications Manager has the other system's certificate installed, it trusts the other system, and communication occurs. If the other system's certificate is not present, the other system is untrusted, and communication fails.

Third-Party CA-Signed Certificates

CA-Signed certificates are trusted third party certificates which signs and issues digital certificates.

By default, Unified Communications Manager uses self-signed certificates for all connections. However, you can add security by configuring a third-party CA to sign certificates. To use a third-party CA, install the CA root certificate chain in Cisco Unified Communications Manager Administration.

To issue CA-signed certificates, submit a Certificate Signing Request (CSR) so that the CA can issue and sign a certificate. For details on how to Upload, Download, and View Certificates, see the **Self-Signed Certificates** section.

Configuration

If you want to use CA-signed certificates from another system connecting to Unified Communications Manager, do the following in Cisco Unified Communications Manager Administration:

- Upload the root certificate chain of the CA that signed the certificates.
- Upload the CA-signed certificates from the other system.

If you want to use CA-signed certificates for Unified Communications Manager:

- Complete a CSR to request CA-signed certificates in Cisco Unified Communications Manager Administration.
- Download both the CA root certificate chain and the CA-signed certificates in Cisco Unified Communications Manager Administration

- Upload both the CA root certificate chain and the CA-signed certificates.

For details on how to obtain and configure root certificates for your CA, see the Certificate Authority documentation.

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		
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.

Server Certificate Types

Server Certificates are basically to identify a server. The server certificates serve the rationale of encrypting and decrypting the content.

Self-signed (own) certificate types in Unified Communications Manager servers are as follows:

Unified Communications Manager imports the following certificate types to the Unified Communications Manager trust store:

Table 3: Certificate Type and Description

Certificate Type	Description
Cisco Unity server or Cisco Unity Connection certificate	Cisco Unity and Cisco Unity Connection use this self-signed root certificate to sign the Cisco Unity SCCP and Cisco Unity Connection SCCP device certificates. For Cisco Unity, the Cisco Unity Telephony Integration Manager (UTIM) manages this certificate. For Cisco Unity Connection, Cisco Unity Connection Administration manages this certificate.
Cisco Unity and Cisco Unity Connection SCCP device certificates	Cisco Unity and Cisco Unity Connection SCCP devices use this signed certificate to establish a TLS connection with Unified Communications Manager.
SIP Proxy server certificate	A SIP user agent that connects via a SIP trunk authenticates to Unified Communications Manager if the CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Unified Communications Manager certificate in its trust store.

Note The certificate name represents a hash of the certificate subject name, which is based on the voice-mail server name. Every device (or port) gets issued a certificate that is rooted at the root certificate.

The following additional trust store exists:

- Common trust store for Tomcat and web applications
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

For more information about CA trust certificates for Cisco Unity Connection, see the Administration Guide for Cisco Unified Communications Manager. These trust-certificates secure connections to Exchange or Meeting Place Express for fetching e-mails, calendar information, or contacts.

Administration Tasks for Certificates

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.

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.
- 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.

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 4: 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.

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.

Update the CTL File

Use this procedure to update the CTL file via a CLI command. If mixed mode is enabled, you must update the CTL file whenever you upload a new certificate.

Procedure

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

Step 2 Run the `utils ctl update CTLFile` command. When the CTL file regenerates, the file gets uploaded to the TFTP server and sent to phones automatically.

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**.