Certificates

Certificate Management

Certificate Management feature provides an overview of the various certificate types, tasks involved to manage certificates, and how to monitor and revoke certificates.

Certificate Overview

Certificates are critical for establishing secure connections in a deployment. They authenticate individuals, computers, and other services on the network. Implementing certificate management provides a good level of protection while reducing complexity.

A Certificate is a file that proves the identity of the certificate owner and contains the following information:

- Certificate Holder Name
- Public Key
- Digital Signature of the Certificate Authority issuing the Certificate

Unified Communications Manager uses certificates that use the Public Key Infrastructure (PKI) to enable encryption and validate server - client identity. It doesn't trust other systems and denies access, unless it has a matching certificate in the appropriate trust store.

Root Certificates secure connections between users and hosts, including devices and application users. Certificates secure and add the client and server identities to the root trust stores.

Administrators can view the fingerprint of server certificates, regenerate self-signed certificates, and delete trust certificates from Unified Communications Manager interface. They can also regenerate and view self-signed certificates using CLI.

For more information on how to update the Unified Communications Manager trust store and manage certificates, see Administration Guide for Cisco Unified Communications Manager.

Note Unified Communications Manager supports only PEM (.pem) and DER (.der) formatted certificates. The maximum size of certificate supported for DER or PEM is 4096 bits.

Note Unified Communications Manager does not support certificates with wildcard entry. For example, "*.cisco.com".

When you upload two certificates, make sure that they have the same name and validity period but different serial numbers and signature algorithms.

For Example,

Root CA with `27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a`serial number and SHA-1 algorithm exists in Unified Communications Manager tomcat-trust.

When you attempt to upload the certificate with `7b:35:33:71:0b:7c:08:b2:47:b3:aa:f9:5c:0d:ca:e4` serial number and SHA-256 algorithm, the certificate management:

- Verifies the incoming certificate validity
- Searches the certificate with the same name in the Tomcat trust folder
- Compares the serial number of the certificate existing in the Tomcat trust folder and the incoming certificate that you're uploading

If the serial numbers are different, it verifies the validity start date of both the certificates. If the start timestamp of the new incoming certificate is the latest, then it replaces the existing certificate else it's not uploaded.

Both SHA-1 and SHA-256 algorithms have same subject name or common name, which implies that they belong to the same entity. The Unified Communications Manager framework doesn't support both these algorithms on the Unified Communications Manager server simultaneously. It supports only one certificate that belongs to any entity in a particular trust folder, irrespective of the signature algorithm.

Certificate Types

This section provides an overview of the different types of certificates and certificate signing request key usage extensions.

Phone Certificate Types

A phone certificate is a unique identifier which authenticates phones. It's crucial for security against IP attacks.

Phone Certificates are as follows:

Table 1:

Phone Certificates	Description
Manufacture Installed Certificate (MIC)	MICs are signed by Cisco Manufacturing CA and we automatically install this certificate in supported Cisco Unified IP Phone. MICs authenticate with CiscoCertificate Authority Proxy Function (CAPF) for Locally Significant Certificates (LSC) installation or download an encrypted configuration file. Cannot use after expiry, as administrators can't modify, delete, or revoke the certificates.
Locally Significant Certificates (LSC)	Cisco Unified IP Phones require an LSC to operate in secure mode and is used for authentication and encryption. They are signed by CAPF, Online or Offline CA and takes precedence over MIC. After you perform the necessary tasks that are associated with CAPF, this certificate gets installed on supported phones. The LSC secures the connection between Unified Communications Manager and the phone after you configure the device security mode for authentication or encryption.

Tip We recommend that you use only MICs for LSC installation. We support LSCs to authenticate the TLS connection with Unified Communications Manager. When phone configurations use MICs for TLS authentication or for any other purpose, we assume no liability as MIC root certificates get easily compromised.

Upgrade Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series to use LSCs for a TLS connection to Unified Communications Manager. Remove MIC root certificates from the Unified Communications Manager trust store to avoid possible future compatibility issues.

Note Phone models that use MICs for TLS connection to Unified Communications Manager may not be able to register.

Administrators should remove the following MIC root certificates from the Unified Communications Manager trust store:

- CAP-RTP-001
- CAP-RTP-002
- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048
- Cisco_Manufacturing_CA_SHA2
- Cisco_Root_CA_M2
- ACT2_SUDI_CA

MIC root certificates that stay in the CAPF trust store get used for certificate upgrades. For information on updating the Unified Communications Manager trust store and managing certificates, see Administration Guide for Cisco Unified Communications Manager.

Note In Unified Communications Manager Release 12.5.1SU2 and earlier, the Secure Onboarding feature doesn't work if you remove the Cisco Manufacturing certificates from the CallManger-trust store, because it can't validate the Manufacture Installed Certificates (MICs) from phones. However, this feature works from Unified Communications Manager Release 12.5.1SU3 onwards, because it uses the CAPF-trust store to validate the MICs from phones.

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 2: 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.

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.

Support for Certificates from External CAs

Unified Communications Manager supports integration with third-party certificate authorities (CAs) by using a PKCS#10 certificate signing request (CSR) mechanism, which is accessible at the Unified Communications Manager GUI.

Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for:

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat

- TVS

Note Multiserver (SAN) CA-signed certificates only applies to nodes in the cluster when the certificate gets uploaded to the Publisher. Generate a new multiserver certificate. Upload it to the cluster every time you add a new node or build it again.

If you run your system in mixed mode, some endpoints may not accept CA certificates with a key size of 4096 or longer. To use CA certificates in mixed mode, choose one of the following options:

- Use certificates with a certificate key size less than 4096.
- Use self-signed certificates.

Note This release of Unified Communications Manager doesn't provide SCEP interface support.

Note Be sure to run the CTL client after you upload a third-party, CA-signed certificate to the platform to update the CTL file.

Restart the appropriate services for the update after running the CTL client.

For example:

- Restart TFTP services and Unified Communications Manager services when you update the Unified Communications Manager certificate.
- Restart CAPF when you update the CAPF certificate.

After uploading the Unified Communications Manager or CAPF certificates, you might observe the phones reset automatically to update their ITL File.

For information on generating Certificate Signing Requests (CSRs) at the platform, see Administration Guide for Cisco Unified Communications Manager.

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 3: 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		

	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
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 4: 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.

Certificate Tasks

This section lists all the procedures to manage certificates.

Bulk Certificate Export

If both the old and new clusters are online at the same time, you can use the Bulk Certificate migration method.

Remember that the Cisco Unified IP Phones verify every downloaded file against either the ITL file, or against a TVS server that exists in the ITL file. If the phone needs to move to a new cluster, the ITL file that the new cluster presents must be trusted by the old cluster TVS certificate store.

Note The Bulk Certificate Export method only works if both clusters are online with network connectivity while the phones are being migrated.

Note During bulk certificate import, you need to import an additional ITLRecovery certificate on both the visiting cluster and the home cluster for Cisco Extension Mobility Cross Cluster (EMCC) to continue functioning. A new option to import ITL_Recovery certificate is added in Bulk Certificate Management for the **Certificate Type** drop-down list.

To use the Bulk Certificate Export method complete the following procedure:

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Security** > **Bulk Certificate Management**.

Step 2 Export certificates from new destination cluster (TFTP only) to a central SFTP server.

Step 3 Consolidate certificates (TFTP only) on the SFTP server using the Bulk Certificate interface.

Step 4 On the origination cluster use the Bulk Certificate function to import the TFTP certificates from the central SFTP server.

Step 5 Use DHCP option 150, or some other method, to point the phones to the new destination cluster.

The phones download the new destination cluster ITL file and attempt to verify it against their existing ITL file. The certificate is not in the existing ITL file so the phone requests the old TVS server to verify the signature of the new ITL file. The phone sends a TVS query to the old origination cluster on TCP port 2445 to make this request.

If the certificate export/consolidate/import process works correctly then the TVS returns success, and the phone replaces the ITL file in memory with the newly downloaded ITL file.

The phones can now download and verify the signed configuration files from the new cluster.

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.

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**.

Certificate Signing Request Fields

Table 5: Certificate Signing Request Fields

Field	Description
Certificate Purpose	From the drop-down list, select a value: - **CallManager**
Distribution	Select a Unified Communications Manager server. When you select this field for multiserver for RSA, the syntax is: `Callmanager common name: <host-name>-ms.<domain>`
	Important Supported from Release 14SU1 onwards. Shows the name of the Unified Communications Manager application that you selected in the **Distribution** field by default.
Auto-populated Domains	This field appears in Subject Alternate Names (SANs) section. It lists the host names that are to be protected by a single certificate.
Parent Domain	This field appears in Subject Alternate Names (SANs) section. It shows the default domain name. You can modify the domain name, if required.
Key Type	This field identifies the type of key used for encryption and decryption for the public-private key pair. Unified Communications Manager supports RSA keys.
Key Length	From the **Key Length** drop-down list, select one of the values. Depending on the key length, the CSR request limits the hash algorithm choices. By having the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. For example, for a key length of 256, the supported hash algorithms are SHA256, SHA384, or SHA512. Similarly, for the key length of 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 can only be selected for RSA certificates. These options aren't available for ECDSA certificates. **Note** Some phone models may fail to register if the RSA **key length** selected for the CallManager **Certificate Purpose** is greater than 2048. From the Unified CM Phone Feature List Report on the Cisco Unified Reporting Tool (CURT), you can check the **3072/4096 RSA key size support** feature for the list of supported phone models.

Field	Description
Hash Algorithm	Select a value from the **Hash Algorithm** drop-down list to have stronger hash algorithm as the elliptical curve key length. From the **Hash Algorithm** drop-down list, select one of the values. **Note** • The values for the **Hash Algorithm** field change based on the value you select in the **Key Length** field. • If your system is running on FIPS mode, it's mandatory that you select SHA256 as the hashing algorithm.

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**.

Generate Self-Signed Certificate

Procedure

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

Step 2 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.

Step 3 Click **Generate Self-Signed Certificate** to generate a new self-signed certificate.
The **Generate New Self-Signed Certificate** window appears.

Step 4 From the **Certificate Purpose** drop-down box, select a system security certificate, such as **CallManager-ECDSA**.

Step 5 Configure the fields in the **Generate New Self-Signed Certificate** window. See the Related Topics section for more information about the fields and their configuration options.

Step 6 Click **Generate**.

Related Topics

Self-Signed Certificate Fields, on page 13

Self-Signed Certificate Fields

Table 6: Self-signed Certificate Fields

Field	Description
Certificate Purpose	Choose the required option from the drop-down list. When you choose any of the following options, the **Key Type** field is automatically set to **`RSA`**. • tomcat • ipsec • ITLRecovery • CallManager • CAPF • TVS When you choose any of the following options, the **Key Type** field is automatically set to **`EC`** (Elliptical Curve). • tomcat-ECDSA • CallManager-ECDSA
Distribution	Choose a Unified Communications Manager server from the drop-down list.
Key Type	This field lists the type of keys used for encryption and decryption of the public-private key pair. Unified Communications Manager supports **EC** and **RSA** key types.

Field	Description
Key Length	Choose any of the following values from the drop-down list: • 1024 • 2048 • 3072 • 4096 Depending on the key length, the self-signed certificate request, limits the hash algorithm choices. With the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. • If the key length value is 256, the supported hash algorithms are SHA256, SHA384, or SHA512. • If the key length value is 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 are chosen only for RSA certificates. These options are not available for ECDSA certificates. **Note** Some phone models might fail to register if the RSA **key length** value chosen for the CallManager **Certificate Purpose** is greater than 2048. For more information, navigate to **Unified CM Phone Feature List Report** on the Cisco Unified Reporting Tool (CURT), to check the **3072/4096 RSA key size support** for the list of supported phone models.
Hash Algorithm	Choose a value that is greater than or equal to the key length from the drop-down list: **Note** • The values in the **Hash Algorithm** drop-down list changes based on the value you have chosen in the **Key Length** field. • If your system is running in FIPS mode, it is mandatory to choose SHA256 as the hashing algorithm.

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 7: 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.

Name	Description	Services to be Restarted
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 CAPF Certificate

To regenerate the CAPF certificate, perform the following steps:

Note If the CAPF certificate is on the publisher, you might observe the phones restarting automatically to update their ITL file. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the CAPF certificate.

Step 2 If you have a CTL file then you must update the CTL file.

For more information see *Regenerate Certificate*, section in the Cisco Unified Communications Manager Security Guide.

Step 3 CAPF service is automatically restarted when CAPF certificate is regenerated.

See the “Activating the Certificate Authority Proxy Function Service” section, in the *Cisco Unified Communications Manager Security Guide*.

Regenerate TVS Certificate

Note If you plan to regenerate both TVS and TFTP certificates, regenerate the TVS certificate, wait for the possible phone restarts to complete, and then regenerate the TFTP certificate. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the TVS certificate.

Step 2 If you have a CTL file then you must update the CTL file.

For more information see *Regenerate Certificate*, section in the Cisco Unified Communications Manager Security Guide.

Step 3 TVS service is automatically restarted when TVS certificate is regenerated.

Regenerate TFTP Certificate

To regenerate a TFTP certificate, follow these steps:

Note If you plan to regenerate multiples certificates you must regenerate the TFTP certificate last. Wait for the possible phone restarts to complete before you regenerate the TFTP certificate. You might need to manually delete the ITL File from all Cisco IP Phones, if you do not follow this procedure. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the TFTP certificate.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If the TFTP service was activated, wait until all the phones have automatically restarted.

Step 3 If your cluster is in mixed mode, update the CTL file.

Step 4 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

System Back-Up Procedure After TFTP Certificate Regeneration

The trust anchor for the ITL File is a software entity: the TFTP private key. If the server crashes, the key gets lost, and phones will not be able to validate new ITL File.

In Unified Communications Manager Release 10.0, the TFTP certificate and private key both get backed up by the Disaster Recovery System. The system encrypts the backup package to keep the private key secret. If the server crashes, the previous certificates and keys will be restored.

Whenever the TFTP certificate gets regenerated, you must create a new system backup. For backup procedures, see the *Administration Guide for Cisco Unified Communications Manager* .

Regenerate ITLRecovery Certificate

Warning Do not regenerate the ITLRecovery Certificate very frequently as this certificate has a long validity with phones and also it contains the CallManager Certificate.

Regenerate ITLRecovery Certificate for Non-Secure Cluster

1. Verify if the ITL File is valid and that all phones in the cluster trust the current ITL File.
2. Regenerate the ITLRecovery Certificate.

   Navigate to the publisher in each cluster to regenerate the ITLRecovery Certificate.

   a. From the Unified OS Administration, choose **Security** > **Certificate Management**

   b. Click **Find**.

      The Certificate List window appears.

   c. Click the ITLRecovery.pem Certificate link from the list of certificates displayed.

   d. Click **Regenerate**, to regenerate the ITLRecovery Certificate.

   e. In the confirmation message pop-up, click **OK**.

3. Sign the ITL file using `utils itl reset localkey` in the CallManager Certificate to accept the new ITL file.
4. Reset in batches all the phones in the cluster.

   Note Make sure all the phones in the cluster are registered.

5. Restart TFTP Service to have the ITL file re-signed by the New ITLRecovery Certificate.

   New ITLRecovery Certificates are uploaded on phones while they reset.

6. Reset in batches all phones in the cluster for a second time to pick up the new ITL File.
7. Phones are uploaded with the new ITLRecovery Certificate after the reset.

Regenerate ITLRecovery Certificate for Secure Cluster

If you want to migrate from a token based ITL file to tokenless ITL file, refer the migration section in security guide.

1. Verify if the ITL File is valid and that all phones in the cluster trust the current ITL File.

2. Verify the CTL File using `show ctl` command.
3. Regenerate the ITLRecovery Certificate.

   Navigate to the publisher in each cluster to regenerate the ITLRecovery Certificate.

   a. From the Unified OS Administration, Choose **Security** > **Certificate Management** > **Find**

   b. Click **Find** to find the list of Certificates.

      The Certificate List window appears.

   c. Click the ITLRecovery.pem Certificate link from the list of Certificates displayed.

   d. Click **Regenerate**, to regenerate the ITLRecovery Certificate.

   e. In the confirmation message pop-up, click **OK**.

4. Sign the CTLFile with `utils ctl reset localkey` in the CallManager Certificate. This also updates the CTLFile with the new ITLRecovery Certificate.
5. Reset in batches all the phones in the cluster to pick up the new CTLFile with new ITLRecovery Certificate.

> **Note**
>
> - Make sure all the phones in the cluster are registered.
> - Regenerating ITLRecovery will affect SAML SSO login of cluster incase system wide certificate is used for enablement.

6. Update the CTLFile to have it re-signed by the new ITLRecovery Certificate `utils ctl update CTLFile`.
7. Reset in batches all phones in the cluster for a second time to pick up the new CTLFile signed by the new ITLRecovery Certificate.
8. Phones are uploaded with the new ITLRecovery Certificate after the reset.

Tomcat Certificate Regeneration

> **Note** When SIP OAuth is enabled, you must restart the Cisco CallManager service after tomcat certificate regeneration and service restart.

To regenerate the Tomcat certificate, perform the following steps:

Procedure

Step 1 Regenerate the Tomcat certificate.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

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.

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.

Interactions and Restrictions

- SIP devices that do not support **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** and **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** can still connect with **TLS_ECDHE_RSA_WITH_AES_256_SHA384**, **TLS_ECDHE_RSA_WITH_AES_128_SHA256**, or **AES128_SHA**. These options are dependent on the TLS cipher option that you choose. If you choose **ECDSA only** option, then the device that does not support the ECDSA ciphers will not be able make a TLS connection to the SIP interface. When you choose the **ECDSA only** option, the value of this parameter are **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** and **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**.
- CTI Manager Secure clients do not support **TLS_ECDHE_RSA_WITH_AES_128_SHA256** , **TLS_ECDHE_RSA_WITH_AES_256_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**, and **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384**. However, they can connect with **AES128_SHA**.

Certificate Monitoring and Revocation

This section allows you to monitor certificates that have to be renewed and revoke certificates which are expired.

Certificate Monitoring Overview

Administrators must be able to track and renew certificates when Unified Communications Manager and IM and Presence Service services contain automated systems. Certificate Monitoring helps administrators know the certificate status on an ongoing basis and email you when a certificate is approaching expiration.

Certificate Monitoring Configuration

The Cisco Certificate Expiry Monitor network service must be running. By default, this service is enabled, but you can confirm if the service is running in Cisco Unified Serviceability application by choosing **Tools** > **Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

Step 1 From the Cisco Unified OS Administration, Choose **Security** > **Certificate Monitor**

Step 2 Enter or choose the configuration details.

Step 3 Click **Save** to save the configuration.

Note By default, the certificate monitor service runs once every 24 hours. 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 doesn't change even when the certificate is close to the expiry date of seven days. It runs every one hour when the certificate either has expired or is going to expire in one day.

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

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**.