



Configuring Authentication and Encryption for CTI, JTAPI, and TAPI

This chapter provides a brief overview of how to secure the CTI, JTAPI, and TAPI applications. It also describes the tasks that you must perform in Cisco Unified CallManager Administration to configure authentication and encryption for the CTI/TAPI/JTAPI application.

This document does not describe how to install the Cisco JTAPI or TSP plug-ins that are available in Cisco Unified CallManager Administration, nor does it describe how to configure the security parameters during the installation. Likewise, this document does not describe how to configure restrictions for CTI-controlled devices or lines.

This chapter provides information on the following topics:

- [Understanding Authentication for CTI, JTAPI, and TAPI Applications](#), page 11-2
- [Understanding Encryption for CTI, JTAPI, and TAPI Applications](#), page 11-3
- [CAPF Overview for CTI, JTAPI, and TAPI Applications](#), page 11-4
- [CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications](#), page 11-5
- [Configuration Checklist for Securing CTI, JTAPI, and TAPI](#), page 11-5
- [Adding Application and End Users to the Security-Related Users Groups](#), page 11-7
- [Activating the Certificate Authority Proxy Function Service](#), page 11-8
- [Updating CAPF Service Parameters](#), page 11-9
- [Finding an Application User or End User CAPF Profile](#), page 11-9
- [Configuring the Application User or End User CAPF Profile](#), page 11-10
- [CAPF Settings in the Application User and End User CAPF Profile Windows](#), page 11-11
- [Deleting an Application User CAPF or End User CAPF Profile](#), page 11-13
- [Configuring JTAPI/TAPI Security-Related Service Parameters](#), page 11-14
- [Viewing the Certificate Operation Status for the Application or End User](#), page 11-14
- [Where to Find More Information](#), page 11-14

Understanding Authentication for CTI, JTAPI, and TAPI Applications

Cisco Unified CallManager 5.0 allows you to secure the signaling connections and media streams between CTIManager and CTI/JTAPI/TAPI applications.



Tip

The following information assumes that you configured security settings during the Cisco JTAPI/TSP plug-in installation. It also assumes that the Cluster Security Mode equals Secure Mode, as configured in the Cisco CTL client. If these settings are not configured when you perform the tasks that are described in this chapter, CTIManager and the application connect via a nonsecure port, port 2748.

CTIManager and the application verify the identity of the other party through a mutually authenticated TLS handshake (certificate exchange); when a TLS connection occurs, CTIManager and the application exchange QBE messages via the TLS port, port 2749.

To authenticate with the application, CTIManager uses the Cisco Unified CallManager self-signed certificate that installs automatically on the Cisco Unified CallManager server during the 5.0 installation; after you install the Cisco CTL client and generate the CTL file, this certificate gets added automatically to the CTL file. Before the application attempts to connect to CTIManager, the application downloads the CTL file from the TFTP server.

The first time that the JTAPI/TSP client downloads the CTL file from the TFTP server, the JTAPI/TSP client trusts the CTL file; because the JTAPI/TSP client does not validate the CTL file, Cisco strongly recommends that the download occur in a secure environment. The JTAPI/TSP client verifies subsequent downloads of the CTL file; for example, after you update the CTL file and the JTAPI/TSP client downloads it from the TFTP server, the JTAPI/TSP client uses the security tokens in the CTL file to authenticate the digital signature of the new file; contents of the file include the Cisco Unified CallManager self-signed certificates and CAPF server certificate.

If the CTL file appears compromised, the JTAPI/TSP client does not replace the downloaded CTL file; the client logs an error and attempts to establish a TLS connection by using an older certificate in the existing CTL file. The connection may not succeed if the CTL file has changed or is compromised. If the CTL file download fails and more than one TFTP server exists, you can configure another TFTP server to download the file, as described in the [“Configuring the Cisco CTL Client”](#) section on page 3-1. The JTAPI/TAPI client does not connect to any port under the following circumstances:

- The client cannot download the CTL file for some reason; for example, no CTL file exists.
- The client does not have an existing CTL file.
- You configured the application user as a secure CTI user.

To authenticate with CTIManager, the application uses a certificate that the Certificate Authority Proxy Function (CAPF) in Cisco Unified CallManager issues. To use TLS for every connection between the application and CTIManager, each instance that runs on the application PC must have a unique certificate. For example, if Cisco Unified CallManager Assistant runs two instances of the service on two different nodes in the cluster, each instance must have its own certificate. One certificate does not cover all instances. To ensure that the certificate installs on the node where Cisco CallManager Assistant service is running, you configure a unique Instance ID for each Application User or End User CAPF Profile in Cisco Unified CallManager Administration, as described in [Table 11-2](#).



Tip

If you uninstall the application from one PC and install it on another PC, you must install a new certificate for each instance on the new PC.

In addition to the tasks that are described in the preceding paragraphs, you must add the application users or the end users to the Standard CTI Secure Connection user group in Cisco Unified CallManager Administration to enable TLS for the application. After you add the user to this group and install the certificate, the application ensures that the user connects via the TLS port.

Understanding Encryption for CTI, JTAPI, and TAPI Applications



Tip

Authentication serves as the minimum requirement for encryption; that is, you cannot use encryption if you have not configured authentication.

Cisco Unified CallManager Assistant, Cisco QRT, and Cisco WebDialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.

If you want to secure the media streams between the application and CTIManager, you must add the application users or the end users to the Standard CTI Allow Reception of SRTP Key Material user group in Cisco Unified CallManager Administration. After the application user and end user(s) get added to this group and the Standard CTI Secure Connection user group and if the cluster security mode equals Secure Mode, CTIManager establishes a TLS connection with the application and provides the key materials to the application in a media event. Although the applications do not record or store the SRTP key materials, the application uses the key materials to encrypt its RTP stream and decrypt the SRTP stream from CTIManager. Be aware that the applications should not record or store the SRTP key materials.

If the application connects to the nonsecure port, port 2748, for any reason, CTIManager does not send the keying material. If CTI/JTAPI/TAPI cannot monitor or control a device or directory number because you configured restrictions, CTIManager does not send the keying material.



Tip

Before the application and end user can use SRTP, verify that the user exists in the Standard CTI Enabled and Standard CTI Secure Connection user groups, which serve as a baseline configuration for TLS. TLS is required for SRTP connections. After the user exists in these groups, you can add the user to the Standard CTI Allow Reception of SRTP Key Material user group. For an application to receive SRTP session keys, the application or end user must exist in three groups: Standard CTI Enabled, Standard CTI Secure Connection, and Standard CTI Allow Reception of SRTP Key Material.

Although Cisco Unified CallManager can facilitate secure calls to and from CTI ports and route points, you must configure the application to support secure calls because the application handles the media parameters. CTI ports/route points register through dynamic or static registration. If the port/route point uses dynamic registration, the media parameters get specified for each call; for static registration, media parameters get specified during registration and cannot change per call. When CTI ports/route points register to CTIManager through a TLS connection, the device registers securely, and the media gets encrypted via SRTP if the application uses a valid encryption algorithm in the device registration request and if the other party is secure.

When the CTI application begins to monitor a call that is already established, the application does not receive any RTP events. For the established call, the CTI application provides a DeviceSnapshot event, which defines whether the media for the call is secure or nonsecure; this event provides no keying material.

CAPF Overview for CTI, JTAPI, and TAPI Applications

Certificate Authority Proxy Function (CAPF), which automatically installs with Cisco Unified CallManager, performs the following tasks for CTI/TAPI/TAPI applications, depending on your configuration:

- Authenticates to the JTAPI/TSP client via an authentication string.
- Issues locally significant certificates (LSC) to CTI/JTAPI/TAPI application users or end users.
- Upgrades existing locally significant certificates.
- Retrieves certificates for viewing and troubleshooting.

When the JTAPI/TSP client interacts with CAPF, the client authenticates to CAPF by using an authentication string; the client then generates its public key and private key pair and forwards its public key to the CAPF server in a signed message. The private key remains in the client and never gets exposed externally. CAPF signs the certificate and then sends the certificate back to the client in a signed message.

You issue certificates to application users or end users by configuring the settings in the Application User CAPF Profile Configuration window or End User CAPF Profile Configuration window, respectively. The following information describes the differences between the CAPF profiles that Cisco Unified CallManager supports:

- **Application User CAPF Profile**—This profile allows you to issue locally significant certificates to secure application users. After you issue the certificate and perform other security-related tasks, a TLS connection opens between the CTIManager service and the application.

One Application User CAPF Profile corresponds to a single instance of the service or application on a server. For example, if you activate a service or application on two servers in the cluster, you must configure two Application User CAPF Profiles, one for each server. If you activate multiple web services or applications on the same server, for example, you must configure two Application User CAPF Profiles, one for each service on the server.

- **End User CAPF Profile**—This profile allows you to issue locally significant certificates to CTI clients. After you issue the certificate and perform other security-related tasks, the CTI client communicates with the CTIManager service via a TLS connection.



Tip

The JTAPI client stores the LSC in Java Key Store format in the path that you configure in the JTAPI Preferences window. The TSP client stores the LSC in an encrypted format in the default directory or in the path that you configure.

The following information applies when a communication or power failure occurs.

- If a communication failure occurs while the certificate installation is taking place, the JTAPI client attempts to obtain the certificate three more times in 30-second intervals. You cannot configure this value.

For the TSP client, you can configure the retry attempts and the retry timer. Configure these values by specifying the number of times that the TSP client tries to obtain the certificate in an allotted time. For both values, the default equals 0. You can configure up to 3 retry attempts by specifying 1 (for one retry), 2, or 3. You can configure no more than 30 seconds for each retry attempt.

- If a power failure occurs while the JTAPI/TSP client attempts a session with CAPF, the client attempts to download the certificate after power gets restored.

CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications

The following requirements exist for CAPF:

- Before you configure the Application User and End User CAPF Profiles, verify that you performed all necessary tasks to install and configure the Cisco CTL client. Verify that the Cluster Security Mode, as configured in the Cisco CTL client, equals Secure Mode.
- To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the first node.
- Because generating many certificates at the same time may cause call-processing interruptions, Cisco strongly recommends that you use CAPF during a scheduled maintenance window.
- Ensure that the first node is functional and running during the entire certificate operation.
- Ensure that the CTI/ JTAPI/TAPI application is functional during the entire certificate operation.

Configuration Checklist for Securing CTI, JTAPI, and TAPI

Table 11-1 provides a list of tasks that you perform to secure the CTI/JTAPI/TAPI application.

Table 11-1 CTI/JTAPI/TAPI Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	<p>Verify that the CTI application and any JTAPI/TSP plug-ins are installed and running.</p> <p>Tip The application user should be assigned to the Standard CTI Enabled group.</p>	<ul style="list-style-type: none"> • Computer Telephony Integration, <i>Cisco Unified CallManager System Guide, Release 5.0</i> • <i>Cisco JTAPI Installation Guide for Cisco Unified CallManager 5.0</i> • <i>Cisco TAPI Installation Guide for Cisco Unified CallManager 5.0</i> • <i>Cisco Unified CallManager Administration Guide, Release 5.0</i>

Table 11-1 CTI/JTAPI/TAPI Security Configuration Checklist (continued)

Configuration Steps	Related Procedures and Topics
<p>Step 2</p> <p>Verify that the following CallManager security features are installed (if not installed, install and configure these features):</p> <ul style="list-style-type: none"> Verify that you installed the CTL client for 5.0 and the CTL file has run so that the CTL file is created. Verify that you installed the CTL provider service and that the service is activated. Verify that you installed the CAPF service and that the service is activated. If necessary, update CAPF service parameters. <p>Tip The CAPF service must run for the Cisco CTL client to include the CAPF certificate in the CTL file. If you updated these parameters when you used CAPF for the phones, you do not need to update the parameters again.</p> <ul style="list-style-type: none"> Verify that the cluster security mode is set to Secure Mode. <p>Tip The CTI/JTAPI/TAPI application cannot access the CTL file if the cluster security mode does not equal Secure Mode.</p>	<ul style="list-style-type: none"> Configuring the Cisco CTL Client, page 3-1 Updating CAPF Service Parameters, page 11-9 <i>Cisco Unified CallManager Administration Guide, Release 5.0</i>
<p>Step 3</p> <p>If you want CTIManager and the application to use a TLS connection, add the application user or end users to the Standard CTI Secure Connection user group.</p> <p>Tip A CTI application can be assigned to either an application user or and end user, but not both.</p>	<p>Adding Application and End Users to the Security-Related Users Groups, page 11-7</p>
<p>Step 4</p> <p>If you want to use SRTP to secure the media streams between CTIManager and the application, add the application user or end user to the Standard CTI Allow Reception of SRTP Key Material user group.</p> <p>Before the application or end user can use SRTP, verify that the user exists in the Standard CTI Enabled and Standard CTI Secure Connection user group, which serves as a baseline configuration for TLS and SRTP connections. After you add the user to these groups, you can add the user to the Standard CTI Allow Reception of SRTP Key Material user group. The application or end user cannot receive SRTP session keys if it does not exist in these three groups.</p> <p>Cisco Unified CallManager Assistant, Cisco QRT, and Cisco WebDialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.</p>	<p>Adding Application and End Users to the Security-Related Users Groups, page 11-7</p> <p>Role Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0</i></p>

Table 11-1 CTI/JTAPI/TAPI Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Configure the Application User CAPF Profile or End User CAPF Profile in Cisco Unified CallManager Administration.	<ul style="list-style-type: none"> • CAPF Overview for CTI, JTAPI, and TAPI Applications, page 11-4 • Configuring the Application User or End User CAPF Profile, page 11-10 • CAPF Settings in the Application User and End User CAPF Profile Windows, page 11-11
Step 6	Enable the corresponding security-related parameters in the CTI/JTAPI/TAPI application.	Configuring JTAPI/TAPI Security-Related Service Parameters , page 11-14

Adding Application and End Users to the Security-Related Users Groups

The Standard CTI Secure Connection user group and the Standard CTI Allow Reception of SRTP Key Material user group display in Cisco Unified CallManager Administration by default. You cannot delete these groups.

If you want the application user or end users to use a TLS connection when communicating with CTIManager, you must add the application user or end users to the Standard CTI Secure Connection user group. A CTI application can be assigned to either an application user or and end user, but not both.

If you want the application and CTIManager to secure the media streams, you must add the application user or end users to the Standard CTI Allow Reception of SRTP Key Material user group.

Before the application and end user can use SRTP, the user must exist in the Standard CTI Enabled and Standard CTI Secure Connection user groups, which serve as a baseline configuration for TLS. TLS is required for SRTP connections. After the user exists in these groups, you can add the user to the Standard CTI Allow Reception of SRTP Key Material user group. For an application to receive SRTP session keys, the application or end user must exist in three groups: Standard CTI Enabled, Standard CTI Secure Connection, and Standard CTI Allow Reception of SRTP Key Material.

Because Cisco Unified CallManager Assistant, Cisco QRT, and Cisco WebDialer do not support encryption, you do not need to add the application users, Unified CMQRTSecureSysUser, IPMASecureSysUser, and the WDSecureSysUser, to the Standard CTI Allow Reception of SRTP Key Material user group.



Tip

For information on deleting an application or end user from a user group, refer to the *Cisco Unified CallManager Administration Guide*. For information about security-related settings in the Role Configuration window, refer to the *Cisco Unified CallManager Administration Guide*.

Procedure

- Step 1** In Cisco Unified CallManager Administration, choose **User Management > User Groups**.
- Step 2** To display all user groups, click **Find**.
- Step 3** Depending on what you want to accomplish, perform one of the following tasks:

- Verify that the application or end users exist in the Standard CTI Enabled group.
- To add an application user or end users to the Standard CTI Secure Connection user group, click the **Standard CTI Secure Connection** link.
- To add an application user or end users to the Standard CTI Allow Reception of SRTP Key Material user group, click the **Standard CTI Allow Reception of SRTP Key Material** link.

Step 4 To add an application user to the group, perform [Step 5](#) through [Step 7](#).

Step 5 Click the **Add Application Users to Group** button.

Step 6 To find an application user, specify the search criteria; then, click **Find**.

Clicking Find without specifying search criteria displays all available options.

Step 7 Check the check boxes for the application users that you want to add to the group; then, click **Add Selected**.

The users display in the User Group window.

Step 8 To add end users to the group, perform step [Step 9](#) through [Step 11](#).

Step 9 Click the **Add Users to Group** button.

Step 10 To find an end user, specify the search criteria; then, click **Find**.

Clicking Find without specifying search criteria displays all available options.

Step 11 Check the check boxes for the ends users that you want to add to the group; then, click **Add Selected**.

The users display in the User Group window.

Additional Information

See the [“Related Topics”](#) section on page 11-14.

Activating the Certificate Authority Proxy Function Service

Cisco Unified CallManager 5.0(2) does not automatically activate the Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability. For information on activating the Certificate Authority Proxy Function service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

To use the CAPF functionality, you must activate this service on the first node. If you did not activate this service before you installed and configured the Cisco CTL client, you must update the CTL file, as described in the [“Updating the CTL File”](#) section on page 3-9.

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific for CAPF. The CAPF certificate, which the Cisco CTL client copies to all servers in the cluster, uses the .0 extension. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications platform GUI.

Updating CAPF Service Parameters

The CAPF Service Parameter window provides information on the number of years that the certificate is valid, the maximum number of times that the system retries to generate the key, the key size, and so on



Tip

Cisco Unified CallManager does not support SCEP or third-party CA-signed LSC certificates, such as Microsoft CA or Keon CA, in this release. Support for third-party certificates is scheduled for a future release. Customers who currently use third-party CA should re-issue a long expiration period (at least 6 months) for their certificates before migration to 5.0 to ensure that certificates will not expire until support for third-party certificates is available.

For the CAPF service parameters to display as Active in Cisco Unified CallManager Administration, you must activate the Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability.



Tip

If you updated the CAPF service parameters when you used CAPF for the phones, you do not need to update the service parameters again.

To update the CAPF service parameters, perform the following procedure:

Procedure

- Step 1** In Cisco Unified CallManager Administration, choose **System > Service Parameters**.
- Step 2** From the Server drop-down list box, choose the first node.
- Step 3** From the Service drop-down list box, choose the Cisco Certificate Authority Proxy Function service. Verify that the word, Active, displays next to the service name.
- Step 4** Update the CAPF service parameters, as described in the help. To display help for the CAPF service parameters, click the question mark or the parameter name link.
- Step 5** For the changes to take effect, restart the Cisco Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability.

Additional Information

See the [“Related Topics” section on page 11-14](#).

Finding an Application User or End User CAPF Profile

To find an application or end user CAPF profile, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager Administration, choose one of the following options, depending on which profile you want to access:

- **User Management > Application User CAPF Profile**
- **User Management > End User CAPF Profile**

The Find and List window displays.

Step 2 From the drop-down list boxes, choose your search criteria for the profiles that you want to list and click **Find**.



Note To find all Application User CAPF Profiles or End User CAPF Profiles that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the profiles that match your search criteria.

Step 3 For the profile that you want to view, click the **Instance ID** link, the **Application User** link (for Application User CAPF Profile only), or the **End User ID** link (for End User CAPF Profile only).



Tip To search for the Instance ID, Application User (for Application User CAPF Profile only), or End User ID (for End User CAPF Profile only) within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the [“Related Topics”](#) section on page 11-14.

Configuring the Application User or End User CAPF Profile

Use [Table 11-2](#) as a reference when you install/upgrade/troubleshoot locally significant certificates for JTAPI/TAPI/CTI applications.



Tip Although the following procedure supports both Application User and End User CAPF Profiles, you cannot configure both types at the same time. Cisco recommends that you configure the Application User CAPF Profile before you configure the End User CAPF Profile.

Procedure

Step 1 In Cisco Unified CallManager Administration, choose one of the following options:

- **User Management > Application User CAPF Profile.**
- **User Management > End User CAPF Profile.**

Step 2 After the Find/List Application User or End User CAPF Profile Configuration window displays, perform one of the following tasks:

- To find an existing Application User or End User CAPF Profile, specify your search criteria and click **Find**.

Clicking Find without specifying search criteria displays all Application User CAPF Profiles or End User CAPF Profiles in the system.

- To add a new Application User or End User CAPF Profile, click **Add New**.

- Step 3** After the CAPF Profile configuration window displays, enter the configuration settings, as described in [Table 11-2](#).
- Step 4** Click **Save**.
- Step 5** Repeat the procedure for each application and end user that you want to use security.

Additional Steps

If you configured the Unified CMQRTSecureSysUser, IPMA SecureSysUser, or WDSecureSysUser in the Application User CAPF Profile Configuration window, you must configure service parameters, as described in the “[Configuring JTAPI/TAPI Security-Related Service Parameters](#)” section on page 11-14.

Additional Information

See the “[Related Topics](#)” section on page 11-14.

CAPF Settings in the Application User and End User CAPF Profile Windows

[Table 11-2](#) describes the CAPF settings in the Application User and End User CAPF Profile windows in Cisco Unified CallManager Administration. For related procedures, see the “[Related Topics](#)” section on page 11-14.

Table 11-2 Application and End User CAPF Profile Configuration Settings

Setting	Description
Application User	For this setting, users that exist in the Application User window display. From the drop-down list box, choose the application user where you want to perform the CAPF operation. This setting does not display in the End User CAPF Profile window.
End User	For this setting, users that exist in the End User window display. From the drop-down list box, choose the end user where you want to perform the CAPF operation. This setting does not display in the Application User CAPF Profile window.

Table 11-2 Application and End User CAPF Profile Configuration Settings (continued)

Setting	Description
Instance ID	<p>Multiple connections (instances) for the application can run in the cluster. To use TLS for every connection between the application and CTIManager, each instance that runs on the application PC (for end users) or server (for application users) must have a unique certificate. For example, if two instances of a service or application run on two servers in the cluster, each instance must have its own certificate.</p> <p>CAPF uses the Application User/End User and Instance ID configuration to determine where to perform the certificate operation. For the application user or end user that you are configuring, enter a unique string by using the following characters: a-z, A-Z, dash (-), underscore (_), or period (.).</p> <p>This field relates to the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter that supports web services and applications. For information on how to access this parameter, see the “Configuring JTAPI/TAPI Security-Related Service Parameters” section on page 11-14.</p>
Certificate Operation	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • No Pending Operation—Displays when no certificate operation is occurring. (default setting) • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate for the application.
Authentication Mode	<p>The authentication mode acts as the method by which the application authenticates with CAPF during the specified certificate operation. By default, Cisco Unified CallManager Administration displays By Authentication String, which installs/upgrades or troubleshoots a locally significant certificate only when the user/administrator enters the CAPF authentication string in the JTAPI/TSP Preferences window.</p>
Authentication String	<p>Manually enter a unique string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits.</p> <p>To install or upgrade a locally significant certificate, the administrator must enter the authentication string in the JTAPI/TSP preferences GUI on the application PC. This string supports one-time use only; after you use the string for the instance, you cannot use it again.</p>
Generate String	<p>If you want CAPF to automatically generate an authentication string, click this button. The 4- to 10-digit authentication string displays in the Authentication String field.</p>
Key Size (bits)	<p>From the drop-down list box, choose the key size for the certificate. The default setting equals 1024. Other options include 512 and 2048.</p> <p>Key generation, which is set at low priority, allows the application to function while the action occurs. Key generation may take up to 30 or more minutes to complete.</p> <p>If you choose a 2048-bit key for the certificate, establishing a connection between the application and Cisco Unified CallManager may take more than 60 seconds. Unless you want to use the highest possible security level, do not configure the 2048-bit key.</p>

Table 11-2 Application and End User CAPF Profile Configuration Settings (continued)

Setting	Description
Operation Completes by	<p>This field, which supports all certificate operations, specifies the date and time by which you must complete the operation.</p> <p>The values that display apply for the first node.</p> <p>Use this setting in conjunction with the CAPF Operation Expires in (days) enterprise parameter, which specifies the default number of days in which the certificate operation must be completed. If you want to do so, you can update this parameter.</p>
Operation Status	<p>This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the specified Certificate Operation. You cannot change the information that displays in this field.</p>

Deleting an Application User CAPF or End User CAPF Profile

This section describes how to delete an Application User CAPF Profile or End User CAPF Profile from the Cisco Unified CallManager database.

Before You Begin

Before you can delete an Application User CAPF Profile or End User CAPF Profile from Cisco Unified CallManager Administration, you must apply a different profile to the devices or delete all devices that use the profile. To find out which devices use the profile, choose **Dependency Records** from the Related Links drop-down list box in the Security Profile Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, refer to the *Cisco Unified CallManager System Guide*.

Procedure

-
- Step 1** Find the Application User CAPF Profile or End User CAPF Profile by using the procedure in the [“Finding an Application User or End User CAPF Profile”](#) section on page 11-9.
- Step 2** To delete multiple profiles, check the check boxes next to the appropriate check box in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.
- Step 3** To delete a single profile, perform one of the following tasks:
- In the Find and List window, check the check box next to the appropriate profile; then, click the **Delete Selected** icon or the **Delete Selected** button.
 - In the Find and List window, click the Name link for the profile. After the specific Application User or End User CAPF Profile Configuration window displays, click the **Delete Selected** icon or the **Delete Selected** button.
- Step 4** When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.
-

Additional Information

See the [“Related Topics”](#) section on page 11-14.

Configuring JTAPI/TAPI Security-Related Service Parameters

After you configure the Application User CAPF Profile or End User CAPF Profile, you must configure the following service parameters for the web service or application:

- CTIManager Connection Security Flag
- CAPF Profile Instance ID for Secure Connection to CTIManager

To access the service parameters, perform the following procedure:

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, choose **System > Service Parameters**.
 - Step 2** From the Server drop-down list box, choose the server where the web service or application is activated.
 - Step 3** From the Service drop-down list box, choose the web service or application:
 - Step 4** After the parameters display, locate the **CTIManager Connection Security Flag** and **CAPF Profile Instance ID for Secure Connection to CTIManager** parameters.
 - Step 5** Update the parameters, as described in the help that displays when you click the question mark or parameter name link.
 - Step 6** Click **Save**.
 - Step 7** Repeat the procedure on each server where the service is activated.
-

Viewing the Certificate Operation Status for the Application or End User

You can view the certificate operation status in a specific Application User or End User CAPF Profile configuration window (not the Find/List window) or in the JTAPI/TSP Preferences GUI window.

Where to Find More Information

Related Topics

- [Configuring the Cisco CTL Client, page 3-1](#)
- [Understanding Authentication for CTI, JTAPI, and TAPI Applications, page 11-2](#)
- [Understanding Encryption for CTI, JTAPI, and TAPI Applications, page 11-3](#)
- [CAPF Overview for CTI, JTAPI, and TAPI Applications, page 11-4](#)
- [CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications, page 11-5](#)
- [Configuration Checklist for Securing CTI, JTAPI, and TAPI, page 11-5](#)

- [Adding Application and End Users to the Security-Related Users Groups](#), page 11-7
- [Activating the Certificate Authority Proxy Function Service](#), page 11-8
- [Updating CAPF Service Parameters](#), page 11-9
- [Finding an Application User or End User CAPF Profile](#), page 11-9
- [Configuring the Application User or End User CAPF Profile](#), page 11-10
- [CAPF Settings in the Application User and End User CAPF Profile Windows](#), page 11-11
- [Deleting an Application User CAPF or End User CAPF Profile](#), page 11-13
- [Configuring JTAPI/TAPI Security-Related Service Parameters](#), page 11-14
- [Viewing the Certificate Operation Status for the Application or End User](#), page 11-14

Related Cisco Documentation

- *Cisco JTAPI Installation Guide for Cisco Unified CallManager*
- *Cisco TAPI Installation Guide for Cisco Unified CallManager*
- *Computer Telephony Integration, Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Administration Guide*

