Authentication and Encryption Setup 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 Unified Communications Manager Administration to configure authentication and encryption for CTI/TAPI/JTAPI applications.

This document does not describe how to install the CiscoJTAPI or TSP plug-ins that are available in Unified Communications Manager 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.

Authentication for CTI, JTAPI, and TAPI Applications

Unified Communications Manager allows you to secure the signaling connections and media streams between CTIManager and CTI/JTAPI/TAPI applications.

Note We assume that you configured security settings during the CiscoJTAPI/TSP plug-in installation. We also assume that the Cluster Security Mode equals Mixed Mode, as configured in the Cisco CTL Client or through the CLI command set **utils ctl**. 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, Port2748.

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 Unified Communications Manager certificate — either the self-signed certificate that installs automatically on the Unified Communications Manager server during installation or a third-party, CA-signed certificate that you uploaded to the platform.

After you generate the CTL file through the CLI command set **utils ctl** or the Cisco CTL Client, this certificate is 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. We recommend that the download occur in a secure environment because the JTAPI/TSP client does not validate the CTL file. The JTAPI/TSP client verifies subsequent downloads of the CTL file; for example, after you update the CTL file, the JTAPI/TSP client uses the security tokens in the CTL file to authenticate the digital signature of the new CTL file it downloads. Contents of the file include the Unified Communications Manager 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. 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) 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. One certificate does not cover all instances. To ensure that the certificate installs on the node whereCisco Unified Communications Manager Assistant service is running, you configure a unique Instance ID for each Application User CAPF Profile Configuration or End User CAPF Profile Configuration in Cisco Unified Communications Manager Administration, as described in CAPF Settings.

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.

You must also add the application users or the end users to the Standard CTI Secure Connection user group in Unified Communications Manager 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.

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.

Unified Communications Manager, Cisco QRT, and Cisco Web Dialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.

To secure the media streams between the application and CTIManager, add the application users or the end users to the Standard CTI Allow Reception of SRTP Key Material user group in Unified Communications Manager. If these users also exist in the Standard CTI Secure Connection user group and if the cluster security mode equals Mixed Mode, CTIManager establishes a TLS connection with the application and provides the key materials to the application in a media event

Note Cluster security mode configures the security capability for your standalone server or cluster.

Although 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.

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 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 Unified Communications Manager can facilitate secure calls to and from CTIports and route points, you must configure the application to support secure calls because the application handles the media parameters.

CTIports/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 CTIports/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.

Stronger Cipher Suites on CTI Ports

When the CTI port registers to CTI Manager through a TLS connection, the device registers securely, and the media gets encrypted through Secure Real-Time Transport Protocol (SRTP) if the application uses a valid encryption algorithm in the device registration request and if the other party is secure.

Unified Communications Manager provides a stronger cipher suite on the Skinny Client Control Protocol (SCCP) interface for CTI ports and allows the secure media notification between the calling and called party. To enable SRTP on CTI ports, CTI application registers by providing supported algorithm IDs of cipher strength.

Unified Communications Manager is enhanced to allow negotiation of these added algorithms on a secure call involving CTI ports:

- CCM_AES_CM_128_HMAC_SHA1_32 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AES_CM_128_HMAC_SHA1_80 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AEAD_AES_128_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_128_COUNTER)

- CCM_AEAD_AES_256_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_256_COUNTER)

When you receive a call, Unified Communications Manager negotiates the media and encryption capabilities as specified by the CTI application while registering the CTI port with those of the called phone. If there is a matching algorithm, the Unified CM sends the key information to both sides to decrypt the packets and monitor or record the media.

Limitations

Unified Communications Manager does not support the CCM_F8_128_HMAC_SHA1_32 and CCM_F8_128_HMAC_SHA1_80 algorithms. If the CTI application tries to register a CTI Port terminating media with these unsupported algorithms, the Unified CM ignores it and selects the best of the remaining available algorithms. If the system does not consist of any algorithm other than these two then the Unified CM will switches to the existing behavior and selects the CCM_AES_CM_128_HMAC_SHA1_32, by default.

CAPF Functions for CTI, JTAPI, and TAPI Applications

Certificate Authority Proxy Function (CAPF), which automatically installs with Unified Communications Manager, 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 applicationusers 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 Unified Communications Manager supports:

- **Application User CAPF Profile**—This profile allows you to issue locally significant certificates to secure application users so that 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. If you activate multiple web services or applications on the same server, you must configure multiple Application User CAPF Profiles, one for each service on the server.

  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.

- **End User CAPF Profile**—This profile allows you to issue locally significant certificates to CTI clients so that 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 the Cluster Security Mode in the **Enterprise Parameters Configuration** window is 1 (mixed mode).
- To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the publisher node.
- Generating many certificates at the same time may cause call-processing interruptions and we recommend that you use CAPF during a scheduled maintenance window.
- Ensure that the publisher node is functional and running during the entire certificate operation.
- Ensure that the CTI/ JTAPI/TAPI application is functional during the entire certificate operation.

Certificate Authority Proxy Function Service Activation

Unified Communications Managerdoes not automatically activate the Certificate Authority Proxy Function service in Cisco Unified Serviceability.

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.

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific to CAPF. The CAPF certificate, which the Cisco CTL Client copies to your standalone server or all server(s) in the cluster, uses the .0 extension. The CAPF certificate is then displayed on the Cisco Unified Communications Operating System GUI as a verification that the CAPF certificate exists.

Set Up Application User or End User CAPF Profile

Use CAPF Settings as a reference when you install/upgrade/troubleshoot locally significant certificates for JTAPI/TAPI/CTI applications.

Tip We recommend that you configure Application User CAPF Profiles before you configure End User CAPF Profiles.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose one of the following options:

a) **User Management** > **User Settings** > **Application User CAPF Profile**

b) **User Management** > **User Settings** > **End User CAPF Profile**.

Step 2 Perform one of the following tasks:

a) To edit an existing profile, click **Find** and select the existing profile.

b) To create a new profile, click **Add New**.

c) To copy settings from an existing profile to a new profile, click **Find** and select the existing profile with the settings that you want. Click **Copy** and name the new profile that will contain those settings. Then edit the new profile as needed.

Step 3 Enter the appropriate settings as described in CAPF Settings.

Step 4 Click **Save**.

Step 5 Repeat this procedure to create additional CAPF Profiles. Create as many profiles as your users need. If you configured the **CCMQRTSecureSysUser**, **IPMASecureSysUser**, or **WDSecureSysUser** in the **Application User CAPF Profile Configuration** window, you must configure **Service Parameters**.

CAPF Settings

The following table describes the CAPF settings in the **Application User CAPF Profile Configuration** and **End User CAPF Profile Configuration** windows.

Table 1: Application and End User CAPF Profile Configuration Settings

Setting	Description
Application User	From the drop-down list, choose the **application user for the CAPF operation**.This setting shows configured application users. This setting does not display in the **End User CAPF Profile** window.
End User ID	From the drop-down list, choose the **end user for the CAPF operation**. This setting shows configured end users. This setting does not display in the **Application User CAPF Profile** window.

Setting	Description
Instance ID	Enter 1-128 alphanumeric characters (a-zA-Z0-9). The Instance ID identifies the user for the certificate operation. You can configure multiple connections (instances) of an application.To secure the connection between the application and CTIManager, ensure that each instance that runs on the application PC (for end users) or server (for application users) has a unique certificate. This field relates to the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter that supports web services and applications.
Certificate Operation	From the drop-down list, choose one of the following options: • **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	The authentication mode for the Install/Upgrade certificate operation specifies By Authentication String, which means CAPF installs/upgrades or troubleshoots a locally significant certificate only when the user/administrator enters the CAPF authentication string in the **JTAPI/TSP Preferences** window.
Authentication String	Manually enter a unique string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install or upgrade a Locally Significant Certificate, you must enter the authentication string in the **JTAPI/TSP preferences** GUI on the applicationPC. This string supports one-time use only; after you use the string for the instance, you cannot use it again.
Generate String	If you want CAPF to automatically generate an authentication string, click the **Generate String** button. The 4- to10-digit authentication string displays in the **Authentication String** field.
Key Order	This field specifies the sequence of the key for CAPF. Select one of the following values from the drop-down list: • **RSA Only** • **EC Only** • **EC Preferred, RSA Backup** **Note** When you add a phone based on the value in **Key Order**, **RSA Key Size**, and **EC Key Size** fields, the device security profile is associated with the phone. If you select the **EC Only** value with the **EC Key Size** value of 256 bits then the device security profile appends with **EC-256** value.

Setting	Description
RSA Key Size (Bits)	From the drop-down list, choose one of the these values—**512**, **1024**, **2048, 3072**, or **4096**.
EC Key Size (Bits)	From the drop-down list, choose one of the these values—**256**, **384**, or **521**.
Operation Completes by	This field, which supports all certificate operations, specifies the date and time by which you must complete the operation. The values displayed apply for the first node. Use this setting with the **CAPF Operation Expires in (days)** enterprise parameter, which specifies the default number of days in which the certificate operation must be completed. You can update this parameter any time.
Certificate Operation Status	This field displays the progress of the certificate operation, such as pending, failed, or successful. You cannot change the information that displays in this field.

Update CAPF Service Parameters

The **Service Parameter** window contains optional settings for the Cisco Certificate Authority Proxy Function. You can configure settings such as the Certificate Issuer, Online CA connection settings, Certificate Validity duration, and key size for the CAPF certificate.

For the CAPF service parameters to display as Active in Cisco Unified Communications Manager Administration, Activate the **Certificate Authority Proxy Function** service in Cisco Unified 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 From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server.

Tip You must choose the publisher node in the cluster.

Step 3 From the **Service** drop-down list, choose the **CiscoCertificate 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 Online 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 Serviceability.

Note For more information on how to configure the Certificate Authority Proxy Function, See **Certificate Authority Proxy Function** chapter.

Delete Application User CAPF or End User CAPF Profile

Before you can delete an Application User CAPF Profile or End User CAPF Profile from Cisco Unified Communications Manager 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 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 System Configuration Guide for Cisco Unified Communications Manager.

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

Procedure

Step 1 Find the Application User CAPF Profile or End User CAPF Profile.

Step 2 Perform one of the following tasks:

a) To delete multiple profiles, check the check boxes next to the appropriate check box in the **Find and List** window; then, click **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

b) To delete a single profile, check the check box next to the appropriate profile In the **Find and List** window; then, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Securing CTI, JTAPI, and TAPI

The following procedure provides the tasks that you perform to secure the CTI/JTAPI/TAPI application.

Procedure

Step 1 Verify that the CTI application and any JTAPI/TSP plug-ins are installed and running.

Tip Assign the application user to the Standard CTI Enabled group.

See the following documentation for more information:

- *Cisco JTAPI Installation Guide for Unified Communications Manager*
- *Cisco TAPI Installation Guide for Unified Communications Manager*

Step 2 Verify that the following Unified Communications Manager security features are installed (if not installed, install and configure these features):

- Verify if the CTL Client is installed and run the CTL file to create it.
- Verify if the CTL provider service is installed and that the service is activated.
- Verify if the CAPF service is installed and that the service is activated. If necessary, update CAPF service parameters.

  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.

- Verify if the cluster security mode is set to Mixed Mode. (Cluster security mode configures the security capability for your standalone server or cluster.)

  Tip The CTI/JTAPI/TAPI application cannot access the CTL file if the cluster security mode does not equal Mixed Mode.

Step 3 Assign your end users and application users to access control groups that contain the permissions they need. Assign your users to all of the following groups so that they can use **TLS** and **SRTP** over CTI connections:

- Standard CTI Enabled
- Standard CTI Secure Connection
- Standard CTI Allow Reception of SRTP Key Material

Tip A CTI application can be assigned to either an application user or an end user, but not both.

The user must already exist in the **Standard CTI Enabled and Standard CTI Secure Connection** user group. The application or end user cannot receive SRTP session keys if it does not exist in these three groups. For more information, see topics related to User access control group configurations.

Note Cisco Unified Communications Manager Assistant, Cisco QRT, and Cisco Web Dialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.

Step 4 Configure CAPF Profiles for your end users and application users. For more information, see **Certificate Authority Proxy Function** chapter.

Step 5 Enable the corresponding security-related parameters in the CTI/JTAPI/TAPI application.

Add Application and End Users to Security-Related Access Control Groups

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

To secure the user connection to CTIManager, you must add the application user or end users to the Standard CTI Secure Connection user group. You can assign a CTI application to either an application user or an 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. SRTP connections require TLS. 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**.

You do not need to add the application users, CCMQRTSecureSysUser, IPMASecureSysUser, and the WDSecureSysUser, to the Standard CTI Allow Reception of SRTP Key Material user group because Cisco Unified Communications Manager Assistant, CiscoQRT, and Cisco Web Dialer do not support encryption.

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

Procedure

Step 1 From Cisco Unified Communications Manager 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:

a) Verify that the application or end users exist in the Standard CTI Enabled group.

b) To add an application user or end users to the **Standard CTI Secure Connection user group**, click the **Standard CTI Secure Connection** link.

c) 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 steps 5 through 7.

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

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 are displayed in the **User Group** window.

Step 8 To add end users to the group, perform steps 9 through 11.

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

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 end users that you want to add to the group; then, click **Add Selected**.

The users are displayed in the **User Group** window.

Set Up 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 **Cisco IP Manager Assistant** service:

- 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 From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server where the **Cisco IP Manager Assistant** service is activated.

Step 3 From the **Service** drop-down list, choose the **Cisco IP Manager Assistant** service.

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.

View Certificate Operation Status for 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.