



Using the Certificate Authority Proxy Function

This chapter provides information on the following topics:

- [Certificate Authority Proxy Function Overview, page 6-2](#)
- [Cisco Unified IP Phone and CAPF Interaction, page 6-2](#)
- [CAPF System Interactions and Requirements, page 6-3](#)
- [Configuring CAPF in Cisco Unified CallManager Serviceability, page 6-4](#)
- [CAPF Configuration Checklist, page 6-4](#)
- [Activating the Certificate Authority Proxy Function Service, page 6-5](#)
- [Updating CAPF Service Parameters, page 6-6](#)
- [Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6](#)
- [CAPF Settings in the Phone Configuration Window, page 6-7](#)
- [Finding Phones Based on LSC Status or Authentication String, page 6-8](#)
- [Generating a CAPF Report, page 6-8](#)
- [Entering the Authentication String on the Phone, page 6-9](#)
- [Where to Find More Information, page 6-10](#)

Certificate Authority Proxy Function Overview

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

- Authenticate via an existing Manufacturing Installed Certificate (MIC), Locally Significant Certificate (LSC), randomly generated authentication string, or optional less secure “null” authentication.
- Issues locally significant certificates to supported Cisco Unified IP Phone models.
- Upgrades existing locally significant certificates on the phones.
- Retrieves phone certificates for viewing and troubleshooting.
- Authenticates via the manufacture-installed certificate.

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.

Cisco Unified IP Phone and CAPF Interaction

When the phone interacts with CAPF, the phone authenticates itself to CAPF using an Authentication String, existing MIC or LSC certificate, or “null”, generates its public key and private key pair and then forwards its public key to the CAPF server in a signed message. The private key remains in the phone and is never exposed externally. CAPF signs the phone certificate and then sends the certificate back to the phone in a signed message.

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

- If a communication failure occurs while the certificate installation is taking place on the phone, the phone will attempt to obtain the certificate three more times in 30-second intervals. You cannot configure these values.
- If a power failure occurs while the phone attempts a session with CAPF, the phone will use the authentication mode that is stored in flash; that is, if the phone cannot load the new configuration file from the TFTP server after the phone reboots. After the certificate operation completes, the system clears the value in flash.



Tip

Be aware that the phone user can abort the certificate operation or view the operation status on the phone.

**Tip**

Key generation, which is set at low priority, allows the phone to function while the action occurs. You may notice that key generation takes up to 30 or more minutes to complete.

Although the phone functions during certification generation, additional TLS traffic may cause minimal call-processing interruptions with the phone; for example, audio glitches may occur when the certificate is written to flash at the end of the installation.

If you choose a 2048-bit key for the certificate, establishing a connection between the phone, Cisco Unified CallManager, and secure SRST-enabled gateway during phone boot-up and failover may take more than 60 seconds. Unless you want the highest possible security level, do not configure the 2048-bit key.

Consider the following information about how CAPF interacts with the Cisco Unified IP Phone 7960 and 7940 when the phone is reset by a user or by Cisco Unified CallManager.

**Note**

In the following examples, if the LSC does not already exist in the phone and if By Existing Certificate is chosen for the CAPF Authentication Mode, the CAPF certificate operation fails.

Example—Nonsecure Device Security Mode

In this example, the phone resets after you configure the Device Security Mode to Nonsecure and the CAPF Authentication Mode to By Null String or By Existing Certificate (Precedence...). After the phone resets, it immediately registers with the primary Cisco Unified CallManager and receives the configuration file. The phone then automatically initiates a session with CAPF to download the LSC. After the phone installs the LSC, configure the Device Support Mode to Authenticated or Encrypted.

Example—Authenticated/Encrypted Device Security Mode

In this example, the phone resets after you configure the Device Security Mode to Authenticated or Encrypted and the CAPF Authentication Mode to By Null String or By Existing Certificate (Precedence...). The phone does not register with the primary Cisco Unified CallManager until the CAPF session ends and the phone installs the LSC. After the session ends, the phone registers and immediately runs in authenticated or encrypted mode.

You cannot configure By Authentication String in this example because the phone does not automatically contact the CAPF server; the registration fails if the phone does not have a valid LSC.

CAPF System Interactions and Requirements

The following requirements exist for CAPF:

- Before you use CAPF, ensure that you performed all necessary tasks to install and configure the Cisco CTL client. To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the first node.
- 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.

- During a certificate upgrade or install operation, if By Authentication String is the CAPF authentication method for the phone, you must enter the same authentication string on the phone after the operation, or the operation will fail. If TFTP Encrypted Configuration enterprise parameter is enabled and you fail to enter the authentication string, the phone may fail and may not recover until the matching authentication string is entered on the phone.
- Cisco strongly recommends that you use CAPF during a scheduled maintenance window because generating many certificates at the same time may cause call-processing interruptions.
- All servers in the Cisco Unified CallManager 5.0(2) cluster must use the same administrator username and password, so CAPF can authenticate to all servers in the cluster.
- Ensure that the first node is functional and running during the entire certificate operation.
- Ensure that the phone is functional during the entire certificate operation.

**Tip**

Cisco IP Telephony Backup and Restore System (BARS) backs up the CAPF data and reports because Cisco Unified CallManager stores the information in the Cisco Unified CallManager database.

Configuring CAPF in Cisco Unified CallManager Serviceability

You perform the following tasks in Cisco Unified CallManager Serviceability:

- Activate the Cisco Certificate Authority Proxy Function service.
- Configure trace settings for CAPF.

Refer to the *Cisco Unified CallManager Serviceability* guides for more information.

CAPF Configuration Checklist

Table 6-1 provides a list of tasks that you perform to install, upgrade, or troubleshoot locally significant certificates.

Table 6-1 CAPF Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	<p>Determine whether a locally significant certificate exists in the phone.</p> <p>Determine whether you need to copy CAP 1.0(1) data to the Cisco Unified CallManager 4.0 publisher database server.</p> <p>Tip If you used the CAPF utility with Cisco Unified CallManager 4.0 and verified that the CAPF data exists in the Cisco Unified CallManager 5.0(2) database, you can delete the CAPF utility that you used with Cisco Unified CallManager 4.0.</p>	<ul style="list-style-type: none"> • Phone documentation that supports your phone model and this version of Cisco Unified CallManager • <i>Data Migration Assistant 2.0 User Guide</i>

Table 6-1 CAPF Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 2	Verify that the Cisco Certificate Authority Proxy Function service is running. Tip This service must run during all CAPF operations. It must also run for the Cisco CTL client to include the CAPF certificate in the CTL file.	Activating the Certificate Authority Proxy Function Service, page 6-5
Step 3	Verify that you performed all necessary tasks to install and configure the Cisco CTL client. Ensure that the CAPF certificate exists in the Cisco CTL file.	Configuring the Cisco CTL Client, page 3-7
Step 4	If necessary, update CAPF service parameters.	<ul style="list-style-type: none"> • Updating CAPF Service Parameters, page 6-6 • Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6
Step 5	To install, upgrade, or troubleshoot locally significant certificates in the phone, use Cisco Unified CallManager Administration.	<ul style="list-style-type: none"> • Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6 • CAPF Settings in the Phone Configuration Window, page 6-7 • Finding Phones Based on LSC Status or Authentication String, page 6-8
Step 6	If it is required for certificate operations, enter the authentication string on the phone.	Entering the Authentication String on the Phone, page 6-9

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.

Activate this service only 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.

To activate the service, perform the following procedure:

Procedure

-
- Step 1** In Cisco Unified CallManager Serviceability, choose **Tools > Service Activation**.
 - Step 2** From the Servers drop-down list box, choose the server on which you want to activate the Certificate Authority Proxy Function service.
 - Step 3** Check the **Certificate Authority Proxy Function** check box.
 - Step 4** Click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 6-10.

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.

For the CAPF service parameters to show Active status in Cisco Unified CallManager Administration, you must activate the Certificate Authority Proxy Function service, as described in [“Activating the Certificate Authority Proxy Function Service”](#) section on page 6-5.

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.
 - Step 4 Update the CAPF service parameters, as described in help that displays for the parameter.



Note To display help for the CAPF service parameters, click the question mark or the parameter name links.

- Step 5 For the changes to take effect, restart the Cisco Certificate Authority Proxy Function service.
-

Additional Information

See the [“Related Topics”](#) section on page 6-10.

Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone

Use [Table 6-2](#) as a reference when you use CAPF.

Perform the following procedure to use the Certificate Authority Proxy Function:

Procedure

-
- Step 1 Find the phone, as described in the *Cisco Unified CallManager Administration Guide*.
 - Step 2 After the search results display, locate the phone where you want to install, upgrade, delete, or troubleshoot the certificate and click the **Device Name (Line)** link for that phone.
 - Step 3 Enter the configuration settings, as described in [Table 6-2](#).
 - Step 4 Click **Save**.

Step 5 Click **Reset**.

Additional Information

See the [“Related Topics” section on page 6-10](#).

CAPF Settings in the Phone Configuration Window

[Table 6-2](#) describes the CAPF settings in the Phone Configuration window in Cisco Unified CallManager Administration. For related procedures, see the [“Related Topics” section on page 6-10](#).

Table 6-2 CAPF Configuration Settings

Setting	Description
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 in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture-installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CallManager creates two trace files, one for each certificate type. <p>By choosing the Troubleshoot option, you can verify that an LSC or MIC exists in the phone.</p> <p>Tip The Delete and Troubleshoot options do not display if a certificate does not exist in the phone.</p>
Authentication String	<p>If you chose the By Authentication String option, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits.</p> <p>To install, upgrade, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.</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>
Operation Completes by	<p>This field, which supports all certificate operation options, specifies the date and time by which you must complete the operation.</p> <p>The values that display apply for the first node.</p>

Table 6-2 CAPF Configuration Settings (continued)

Setting	Description
Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot certificate operation options. You cannot change the information that displays in this field.

Finding Phones Based on LSC Status or Authentication String

To find phones based on the certificate operation status or the authentication string, perform the following procedure:

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, choose **Device > Phone**.
- Step 2** From the Find Phone where drop-down list box, choose one of the following options:
- **LSC Status**—Choosing this option returns a list of phones that use CAPF to install, upgrade, delete, or troubleshoot locally significant certificates.
 - **Authentication String**—Choosing this option returns a list of phones with an authentication string that is specified in the Authentication String field.
- Step 3** If you want to do so, specify additional search criteria for the LSC status or authentication string by choosing an option in the drop-down list box next to the Find Phone Where drop-down list box; then, enter the specific search criteria.
- Step 4** After you specify your search criteria, click **Find**.



Tip To search for additional information within the search results, check the **Search Within Results** check box, enter your search criteria, and click **Find**.

Additional Information

See the [“Related Topics” section on page 6-10](#).

Generating a CAPF Report

If you want to do so, you can generate a CAPF report to view the status of the certificate operation, the authentication string, security profile, authentication mode, and so on. The report includes information such as device name, device description, security profile, authentication string, authentication mode, LSC status, and so on.

To generate a CAPF report, perform the following procedure:

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, choose **Device > Phone**.
The Find/List window displays.
- Step 2** In the Find Phone Where drop-down list box, choose one of the following options:
- Device Name
 - Device Description
 - LSC Status
 - Authentication String
 - Security Profile



Tip If you want to do so, specify additional search criteria by choosing an option in the drop-down list box next to the Find Phone Where drop-down list box; then, enter the specific search criteria.

The search results display.



Tip To search for additional information within the search results, check the **Search Within Results** check box, enter your search criteria, and click **Find**.

- Step 3** In the Related Links drop-down list box, choose **CAPF Report in File**; then, click **Go**.
- Step 4** Save the file to a location that you will remember.
- Step 5** Use Microsoft Excel to open the .csv file.
-

Additional Information

See the [“Related Topics” section on page 6-10](#).

Entering the Authentication String on the Phone

If you chose the By Authentication String mode and generated an authentication string in Cisco Unified CallManager, you must enter the authentication string on the phone before the locally significant certificate installation occurs.



Tip

The authentication string applies for one-time use only. Obtain the authentication string that displays in the Phone Configuration window or in the CAPF report. For information on how to enter the authentication string on the phone, refer to the phone documentation that supports your phone model and this version of Cisco Unified CallManager.

Before you enter the authentication string on the phone, verify that the following conditions are met:

- The CAPF certificate exists in the CTL file.
- You activated the Cisco Certificate Authority Proxy Function service, as described in [“Activating the Certificate Authority Proxy Function Service” section on page 6-5](#).

- The first node is functional and running. Ensure that the server runs for each certificate installation.
- A signed image exists on the phone; refer to the Cisco Unified IP Phone administration documentation that supports your phone model.

Additional Information

See the [“Related Topics”](#) section on page 6-10.

Where to Find More Information

Related Topics

- [Certificate Authority Proxy Function Overview, page 6-2](#)
- [Cisco Unified IP Phone and CAPF Interaction, page 6-2](#)
- [CAPF System Interactions and Requirements, page 6-3](#)
- [Configuring CAPF in Cisco Unified CallManager Serviceability, page 6-4](#)
- [CAPF Configuration Checklist, page 6-4](#)
- [Activating the Certificate Authority Proxy Function Service, page 6-5](#)
- [Updating CAPF Service Parameters, page 6-6](#)
- [Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6](#)
- [CAPF Settings in the Phone Configuration Window, page 6-7](#)
- [Finding Phones Based on LSC Status or Authentication String, page 6-8](#)
- [Generating a CAPF Report, page 6-8](#)
- [Entering the Authentication String on the Phone, page 6-9](#)

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

Cisco Unified CallManager Serviceability