



Activating the Certificate Authority Proxy Function Server

Revised: November 2014, OL-18391-01



Tip

When performing the tasks in this chapter, it can be helpful to keep two browser sessions open, with one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Multipoint Switch (CTMS) administration interface.

Contents

This chapter describes how to activate the CAPF server and includes the following sections:

- [CAPF Server Activation Task Checklist, page 1-1](#)
- [Activating the CAPF Server, page 1-2](#)
- [Creating and Configuring an Application User, page 1-4](#)
- [Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates from the Phone, page 1-11](#)
- [Finding Phones on Basis of LSC Status or Authentication String, page 1-12](#)
- [Managing CAPF Settings in the Phone Configuration Window, page 1-13](#)
- [Entering the CAPF Authentication String Using CLI, page 1-14](#)
- [Where to Go Next, page 1-14](#)

CAPF Server Activation Task Checklist

[Table 1-1](#) provides a list of configuration tasks that you perform to activate CAPF Server for the first time.

Table 1-1 Cisco CAPF Server Activation Task Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Enable secure communications between Cisco Unified CM and Cisco TelePresence devices	Activating the CAPF Server, page 1-2.
Step 2	Create and configure an application user	Creating and Configuring an Application User, page 1-4
Step 3	Configure a CAPF profile on the server side and client side.	Creating a CAPF Profile for Cisco Unified CM, page 1-6
Step 4	Download the CAPF certificates from Cisco Unified CM	Downloading Certificates from Cisco Unified CM, page 1-9
Step 5	Enter the CAPF authentication string using command-line interface (CLI) to install the locally significant certificate (LSC).	Entering the CAPF Authentication String Using CLI, page 1-14

Activating the CAPF Server

Use the information in this section to enable secure communications between Cisco Unified CM and Cisco TelePresence devices. The CAPF Server is installed by default with Cisco Unified CM and runs as a service; after you activate and start the CAPF service, Cisco Unified CM is used as a CAPF server. You can then configure the CTMS, and Cisco TelePresence Manager (CTS-Manager) software as CAPF clients.



Note

To enable secure conference bridge registration, set the Cisco Unified CM cluster security mode to mixed mode: **Cluster Security Mode** field is set to **1**. Mixed mode allows authenticated, encrypted, and nonsecure Cisco Unified IP Phones to register with Cisco Unified Communications Manager. In this mode, Cisco Unified Communications Manager ensures that authenticated or encrypted devices use a secure port.

Cisco Unified Communications Manager disables auto-registration if you configure mixed mode.

To activate the CAPF server, follow these steps:

Step 1 Log in to Cisco Unified CM administration interface.



Note

If there are Cisco Unified CM subscribers in your cluster, perform this step for your Cisco Unified CM publisher. You configure the subscribers later in this chapter.

Step 2 From the Navigation drop-down list, choose **Cisco Unified Serviceability** and click **Go**.

Step 3 Choose **Tools > Service Activation**.

Step 4 Choose a server from the Server drop-down list and click **Go**.

Step 5 Scroll down to the Security Services area and check the **Cisco Certificate Authority Proxy Function** check box to activate the CAPF server, as shown in [Figure 1-1](#).

Figure 1-1 Activating the CAPF service in Cisco Unified CM

The screenshot displays the Cisco Unified CallManager Serviceability interface. The page title is "Cisco Unified CallManager Serviceability" with the subtitle "For Cisco Unified Communications Solutions". The user is logged in as "ccadministrator". The "Service Activation" section is active, showing a status of "Ready". The "Select Server" dropdown is set to "vijendra-cm5".

The "CM Services" section is expanded, showing a table of services:

Service Name	Activation Status
Performance and Monitoring Services	
<input checked="" type="checkbox"/> Cisco Serviceability Reporter	Activated
<input checked="" type="checkbox"/> Cisco CallManager SNMP Service	Activated
Security Services	
<input checked="" type="checkbox"/> Cisco CTL Provider	Activated
<input checked="" type="checkbox"/> Cisco Certificate Authority Proxy Function	Activated
Directory Services	
<input type="checkbox"/> Cisco DirSync	Deactivated

At the bottom of the page, there are buttons for "Save", "Set to Default", and "Refresh". An information icon indicates that an asterisk (*) denotes a required item.

274402

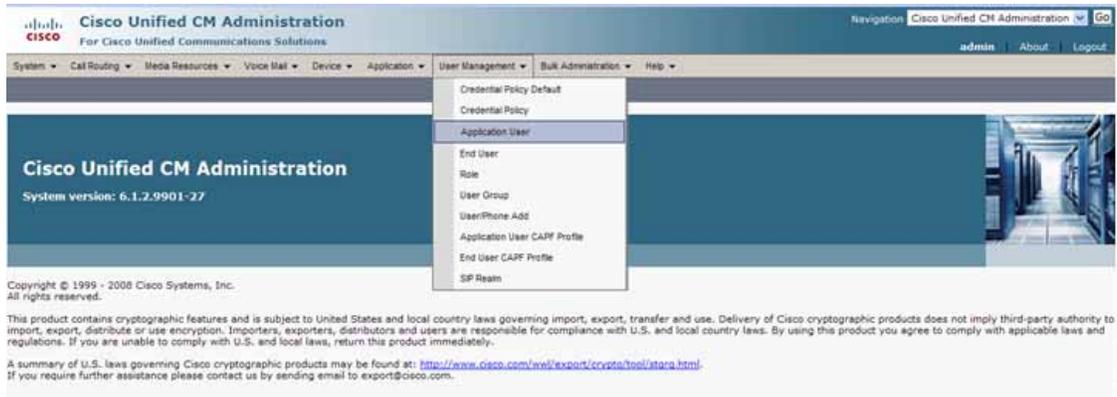
Step 6 Proceed to [Creating and Configuring an Application User](#).

Creating and Configuring an Application User

To create and configure an application user, or to modify the configuration of an existing user, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **User Management > Application User**, as shown in [Figure 1-2](#).

Figure 1-2 Creating an Application User



- Step 2** Choose one of the following:

- To create a new CTMS application user, click the **Add New** button, and continue to [Step 3](#).



Note Cisco recommends that you create a new application user for each system component (CTMS, CTRS, and CTS-Manager.)

- To use an existing application user, click the **Find** button, locate the user ID, click the hypertext link to select that user, and continue to [Step 4](#).

Step 3 In the **Application User Information** area, enter a user ID and password, as shown in [Figure 1-3](#).



Note Make a note of the user ID that you create.

Figure 1-3 Adding Application User ID and Password

Application User Configuration

Save Delete Copy Add New

Status

Status: Ready

Application User Information

User ID* dhsr110

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

Presence Group* Standard Presence group

274405

Step 4 Add and verify the following groups and roles in the Permissions Information area:

- a. Click **Add to User Group**.
- b. Check the check box next to **Standard CTI Enabled** and **Standard CTI Secure Connection**.
- c. Click **Add Selected**.
Cisco Unified CM automatically adds the information that you choose in the Groups field to the Roles field.
- d. Verify that the following roles display in the Roles field:
 - Standard AXL API Access
 - Standard CCM Admin Users
 - Standard CTI Enabled
 - Standard CTI Secure Connection
- e. If the Standard AXL API Access and Standard CCM Admin Users roles do not appear in the Roles field, you can add them now.

Choosing this permission information enables the following security features in Cisco Unified CM:

- Transport Layer Security (TLS) support
- Certificate Tracking (in this case, the LSC)
- For Cisco Unified CM Version 7.0, Secure Real-Time Protocol (SRTP) support

Creating a CAPF Profile for Cisco Unified CM

A CAPF Server authenticates a CAPF Client based on a client profile pre-configured in the Cisco Unified CM database. This requires users to configure a CAPF Profile on the server side and client side. The CAPF Profile parameters need to be provided to authenticate each client. The CAPF Server configuration is performed from the Cisco Unified CM Administration web page which allows users to configure an Application or End-user CAPF Profile. This configuration record is stored in the server database to authenticate the client which is trying to download the certificate.

To create a CAPF profile, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **User Management > Application User CAPF Profile**, as shown in [Figure 1-4](#).

Figure 1-4 Creating a CAPF Profile



Step 2 Click the **Add New** button, as shown in [Figure 1-5](#).

Figure 1-5 Adding a New User



Step 3 Enter the following information using [Figure 1-6](#) as a guide:

- **Application User**—Select the user you just created in the “[Creating and Configuring an Application User](#)” section on page 1-4.
- **Instance Id**—Enter an ID that is unique for this Cisco Unified CM cluster.



Note Make a note of the Instance ID that you create. You use this information later in this chapter when you download LSCs in the “[Downloading LSCs onto an Infrastructure Device](#)” section on page 3-5.

- **Certificate Operation**—Choose **Install//Upgrade**.
- **Authentication Mode**—Choose **By Authentication String** (default).
- **Authentication String**—Click this text box and manually enter an authentication string. Optionally, you can click the **Generate String** button to create a randomly generated authentication string.



Note Make a note of the authentication string. You use this information later in this chapter.

- **Key size (bits)**—Choose **1024** (default).
- **Operation Completes By**—Leave the default value.



Note To avoid regenerating a new authentication string, complete the procedure in the “[Downloading LSCs onto an Infrastructure Device](#)” section on page 3-5 before the date and time that is specified in the Operation Completes By field.

Figure 1-6 Configuring the CAPF Profile

Application User CAPF Profile Configuration

Save

Status

Status: Ready

Application User CAPF Profile

Application User* -- Not Selected --

Instance Id*

Certificate Authority Proxy Function (CAPF) Information

Certificate Operation* Install/Upgrade

Authentication Mode* By Authentication String

Authentication String

Key Size (bits)* 1024

Operation Completes By 2008 : 10 : 2 : 12 (YY:MM:DD:HH)

Certificate Operation Status: None

Generate String

Save

* - indicates required item

Done

274409

- Step 4** Click **Save**. The Application User CAPF Profile Configuration window should look similar to the example in [Figure 1-7](#).

Figure 1-7 Application User CAPF Profile Configuration Window Example

Application User CAPF Profile Configuration

Save Delete Copy Add New

Status
 Status: Ready

Application User CAPF Profile
 Application User* dh93-User
 Instance Id* 093

Certification Authority Proxy Function (CAPF) Information
 Certificate Operation* Install/Upgrade
 Authentication Mode* By Authentication String
 Authentication String 1410254971 **Generate String**
 Key Size (bits)* 1024
 Operation Completes By 2008 : 10 : 5 : 12 (YY:MM:DD:HH)
 Certificate Operation Status: Upgrade Success

Save Delete Copy Add New

274410

Downloading Certificates from Cisco Unified CM

Download the Certificates from Cisco Unified CM in preparation for uploading them to CTMS and Cisco TelePresence Manager. To download the certificate(s), follow these steps:

- Step 1** Log in to Cisco Unified CM administration interface.

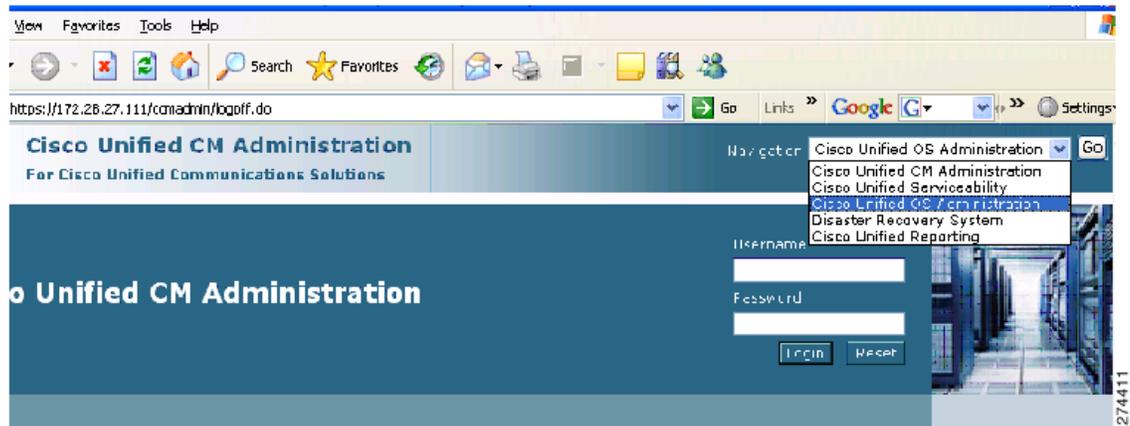


Note

If there are Cisco Unified CM subscribers in your cluster, perform this step for your Cisco Unified CM publisher. You configure the subscribers later in this procedure.

- Step 2 From the Navigation drop-down list, choose **Cisco Unified OS Administration** and click **Go**, as shown in Figure 1-8.

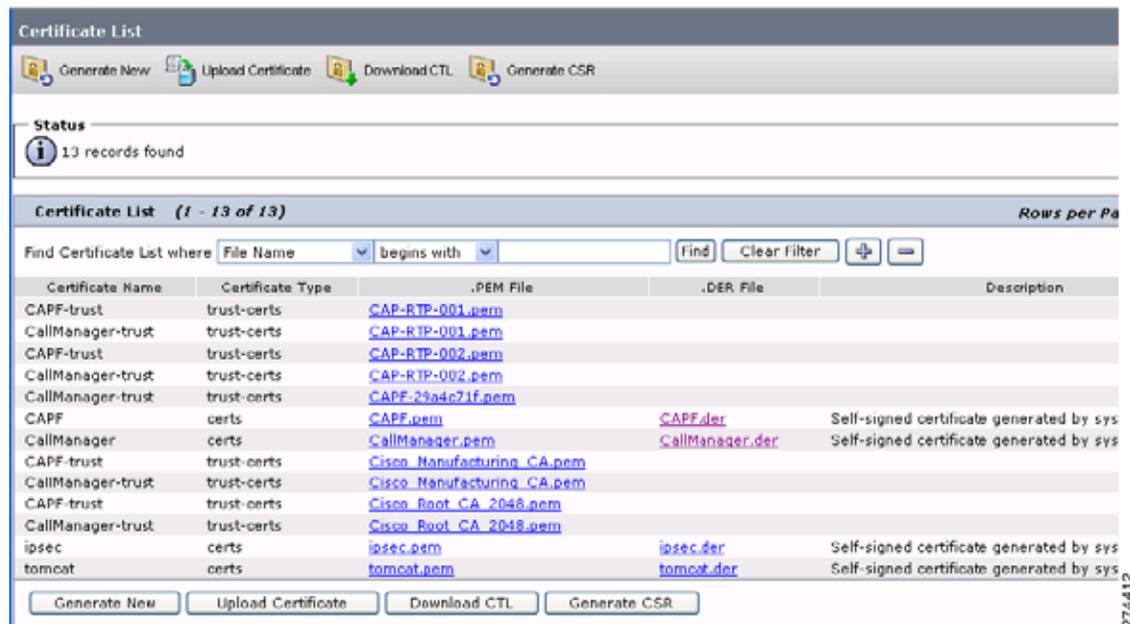
Figure 1-8 Navigating to the Cisco Unified OS Administration Page



- Step 3 Choose **Security > Certificate Management**. The Certificate List window appears, as shown in Figure 1-9.

- Step 4 Click the **Find** button.

Figure 1-9 Location of CAPF.der File in Find Results



- Step 5 Locate the CAPF.der file and click the **CAPF.der** hypertext link. The Certificate Configuration window appears.

- Step 6 Click **Download**.

- Step 7 Download the file to your local machine, retaining the **CAPF.der** file name.

- Step 8** Return to the Certificate List window.
- Step 9** If you cannot locate the CallManager.der file, click the **Find** button.
- Step 10** Locate the CallManager.der file and click the **CallManager.der** hypertext link.
- Step 11** Click **Download**.
- Step 12** Download the file to your local machine. Rename the file to **CUCM0.der**.



Note Be sure to rename this file.

- Step 13** If there are any subscribers in your Cisco Unified CM cluster, do the following:
- Download the CallManager.der file from each subscriber to your local machine by performing [Step 1](#) through [Step 11](#).
 - For each subscriber, rename the CallManager.der file to **CUCM x .der**, where x is the number of the subscriber. For example:

Download the CallManager.der file from the first subscriber and rename that file **CUCM1.der**, download the CallManager.der file from the second subscriber and rename that file **CUCM2.der**, and so on.
-

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

To use the Certificate Authority Proxy Function, follow these steps, using the information in [Table 1-2](#) as a reference:

-
- Step 1** Find the phone, as described in the *Cisco Unified Communications Manager 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 1-2](#).
- Step 4** Click **Save**.
- Step 5** Click **Reset**.
-

Finding Phones on Basis of LSC Status or Authentication String

To find phones on the basis of certificate operation status or the authentication string, follow these steps:

-
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
The Find and List window displays. Records from an active (prior) query may also display in the window.
- Step 2** From the first 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** From the second drop-down list box, choose a search pattern.
- Step 4** Specify the appropriate search text, if applicable.



Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

- Step 5** Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.
- Step 6** From the list of records that display, click the link for the record that you want to view.



Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Managing CAPF Settings in the Phone Configuration Window

Table 1-2 describes the CAPF settings in the Phone Configuration window in Cisco Unified Communications Manager Administration.

Table 1-2 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 Communications Manager creates two trace files, one for each certificate type. <p>Tip By choosing the Troubleshoot option, you can verify that an LSC or MIC exists in the phone. 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. See “Entering the CAPF Authentication String Using CLI” section on page 1-14 for more information.</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>
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 Install/Upgrade, Delete, or Troubleshoot certificate operation options. You cannot change the information that displays in this field.</p>

Entering the CAPF Authentication String Using CLI

If you chose the By Authentication String mode and generated an authentication string, you must enter the authentication string using CTS command-line interface (CLI) to install the locally significant certificate (LSC).



Tip

The authentication string is for one-time use only.

Before You Begin

Before you enter the authentication string using CLI, 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 CAPF Server” section on page 1-2](#).
- The Cisco Unified CM server is operational.

Procedure

To set the authentication string using CLI, follow these steps:

Step 1 Log into your SSH client.

Step 2 Enter the following command:

```
admin help set security authstring
```

```
authstring help:
This will set the CAPF authentication string.
```

```
syntax is: set security authstring numeric_string
```

```
numeric_string      mandatory      This is a numeric authorization
                                string that matches the CUCM device
                                setting
```

Note: The authentication string must be greater than four digits and numerical in value.

Example:

```
admin: set security authstring 123456
admin:
```

Related Information

See the [Cisco Unified Communications Manager Security Guide](#) for step-by-step instructions for configuring authentication and encryption for Cisco Unified Communications Manager and Cisco Unified IP Phones.

Where to Go Next

See [Chapter 2, “Configuring the Cisco CTL Client”](#) for information about the Certificate Trust List (CTL) file.