Certificate Authority Proxy Function

This chapter provides information about the certificate authority proxy function.

- About Certificate Authority Proxy Function, on page 1
- Cisco IP Phone and CAPF Interaction, on page 2
- CAPF Interaction with IPv6 Addressing, on page 3
- CAPF System Interactions and Requirements, on page 6
- CAPF in Cisco Unified Serviceability Setup, on page 7
- Set Up CAPF, on page 7
- Activate Certificate Authority Proxy Function Service, on page 7
- Update CAPF Service Parameters, on page 8
- Generate and Import Third Party CA-Signed LSCs, on page 8
- Install, Upgrade, Troubleshoot, or Delete Certificates From Phone Using CAPF, on page 9
- CAPF Settings, on page 10
- Find Phones by LSC Status or Authentication String, on page 11
- Generate CAPF Report, on page 12
- Enter Phone Authentication String, on page 13
- Verify Phone Authentication String, on page 14

About Certificate Authority Proxy Function

Certificate Authority Proxy Function (CAPF), which automatically installs with Cisco Unified Communications Manager, 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 IP Phones.
- Upgrades existing locally significant certificates on the phones.
- Retrieves phone certificates for viewing and troubleshooting.

During installation, a certificate that is specific for CAPF gets generated. This CAPF certificate, which the Cisco CTL Client copies to all Cisco Unified Communications Manager servers in the cluster, uses the.0 extension.

Cisco IP Phone and CAPF Interaction

When the phone interacts with CAPF, the phone authenticates itself to CAPF by 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 never gets exposed externally. CAPF signs the phone certificate and then sends the certificate back to the phone in a signed message.

Beginning from Cisco Unified Communications Manager Release 11.5(1) SU1, all the LSC certificates issued by CAPF service are signed with SHA-256 algorithm. Therefore, Cisco IP Phones 6900, 7800, 7900, 8800, 8900, and 9900 series models supports SHA-256 signed LSC certificates and external SHA2 identity certificates (Tomcat, CallManager, CAPF, TVS, and so on). For any other cryptographic operation that require validation of signature, only SHA-1 is supported.

Note We recommend to use the Cisco Unified Communications Manager prior to 11.5(1) SU1 release. If you use phone the models, which are in End of Software Maintenance or End of Life.

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.

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

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 Communications Manager 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 Security 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 Communications Manager 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 Interaction with IPv6 Addressing

CAPF can issue and upgrade certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. To issue or upgrade certificates for phones that are running SCCP that use an IPv6 address, you must set the Enable IPv6 service parameter to **True** in Unified Communications Manager Administration.

When the phone connects to CAPF to get a certificate, CAPF uses the configuration from the Enable IPv6 enterprise parameter to determine whether to issue or upgrade the certificate to the phone. If the enterprise parameter is set to **False**, CAPF ignores/rejects connections from phones that use IPv6 addresses, and the phone does not receive the certificate.

The following table describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

Table 1: How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Dual-stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv6	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv4	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6	IPv6	IPv4	Phone cannot connect to CAPF.

Table 2: How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Two stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Two stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Two stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4	IPv6	Phone cannot connect to CAPF.
Two stack	IPv6	IPv4	Phone cannot connect to CAPF.
Two stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4 stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
IPv4 stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4 stack	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6 stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6 stack	IPv6	IPv4	Phone cannot connect to CAPF.

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 CiscoCTL Client. To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the first node.
- 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.
- 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.
- If a secure phone gets moved to another cluster, the Cisco Unified Communications Manager will not trust the LSC certificate that the phone sends because it was issued by another CAPF, whose certificate is not in the CTL file. To enable the secure phone to register, delete the existing CTL file. You can then use the Install/Upgrade option to install a new LSC certificate with the new CAPF and reset the phone for the new CTL file (or use the MIC). Use the Delete option in the CAPF section on the Phone Configuration window to delete the existing LSC before you move the phones.

Tip CiscoIP Telephony Backup and Restore System (BARS) backs up the CAPF data and reports because Cisco Unified Communications Manager stores the information in the Cisco Unified Communications Manager database.

CAPF in Cisco Unified Serviceability Setup

You perform the following tasks in Cisco Unified Serviceability:

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

Refer to the *Cisco Unified Serviceability Administration Guide*s for more information.

Set Up CAPF

Perform the following tasks to install, upgrade, or troubleshoot locally significant certificates.

Procedure

Step 1 Determine whether a locally significant certificate exists in the phone.

Determine whether you need to copy CAPF data to the Unified Communications Manager publisher database server. For more information, see the *Cisco IP Phone Administration Guide* for your phone model.

.

Tip If you used the CAPF utility with Unified Communications Manager 4.0 and verified that the CAPF data exists in the Unified Communications Manager database, you can delete the CAPF utility that you used with Unified Communications Manager 4.0.

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 CiscoCTL Client to include the CAPF certificate in the CTL file.

Step 3 Verify that you performed all necessary tasks to install and configure the CiscoCTL Client. Ensure that the CAPF certificate exists in the CiscoCTL file.

Step 4 If necessary, update CAPF service parameters.

Step 5 To install, upgrade, or troubleshoot locally significant certificates in the phone, use Unified Communications Manager Administration.

Step 6 If it is required for certificate operations, enter the authentication string on the phone.

Activate Certificate Authority Proxy Function Service

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

If you did not activate this service before you installed and configured the Cisco CTL Client, you must update the CTL file. Activate this service only on the first node.

To activate the service, perform the following procedure:

Procedure

Step 1 In Cisco Unified 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**.

Update 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, and so on.

For the CAPF service parameters to show Active status in Cisco Unified Communications Manager Administration, you must activate the Certificate Authority Proxy Function service.

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

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

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

Tip You must choose the first node in the cluster.

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

Generate and Import Third Party CA-Signed LSCs

CAPF LSCs are locally signed. However, you may require phones to use third party CA signed LSCs.

Note Perform Steps 1 and 2 once and repeat the remaining steps until you configure all require phone LSC operations.

Procedure

Step 1 Import the third party CA certificate into the Unified Communications Manager trust store.

Step 2 Follow these steps to configure the service parameter Certificate Issuer to Endpoint:

a) In Cisco Unified CM Administration, select **System** > **Service Parameter**.
b) Select your Unified Communications Manager server frop the drop-down list box.
c) Under the service drop-down list box, select **Cisco Certificate Authority Proxy Function**.
d) For the service parameter Certificate Issuer to Endpoint, select **Offline CA**.

Step 3 Check CSR generation progress. After the phones reregister, use the CLI command **utils capf csr count**to check whether the CSRs are generated.

Step 4 Dump the CSRs to the desired location (local directory or remote directory through FTP or TFTP) by using the CLI command **utils capf csr dump**.
The CLI tars and zip the CSRs into a single file (`.tgz`) before uploading.

Step 5 When all the signed certificates are provided by the CA, you need to tar and zip all the certificates into a single file using the Linux command **`tar cvzf <filename.tgz> *.der`**.

Step 6 Use the CLI command **utils capf cert import** to import the certificates into Unified Communications Manager.

Note The imported certificate must be in DER format, and they must be tarred in a flat file structure.

The CLI command untars the file, and parses and verifies each certificate. If the certificates are valid, they are sent to the phones, and the corresponding CSR is deleted.

What to do next

To remove all the CSRs and certificates that were previously built and imported, you can use the command **utils capf csr delete**.

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

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

Procedure

Step 1 Find the phone, as described in the *Administration Guide for Cisco Unified Communications Manager* .

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 3: CAPF Configuration Settings, on page 10.

Step 4 Click **Save**.

Step 5 Click **Reset**.

CAPF Settings

The following table describes the CAPF settings in the **Phone Configuration** window in Cisco Unified Communications Manager Administration.

Table 3: CAPF Configuration Settings

Setting	Description
Certificate Operation	From the drop-down list box, 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 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. **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.
Authentication String	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. To install, upgrade, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.
Generate String	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.

Setting	Description
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.
RSA Key Size (Bits)	From the drop-down list box, choose one of the these values—**512**, **1024**, or **2048**.
EC Key Size (Bits)	From the drop-down list box, choose one of the these values—**256**, **384**, or **521**.
Operation Completes by	This field, which supports all certificate operation options, specifies the date and time by which you must complete the operation. The values that display apply for the first node.
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.

Find Phones by LSC Status or Authentication String

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

Procedure

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:

a) **LSC Status**— Choosing this option returns a list of phones that use CAPF to install, upgrade, delete, or troubleshoot locally significant certificates.
b) **LSC Expires**- Choosing this option returns a list of phones based on the specified lsc expiration search criteria.
c) **LSC Issued by** - Choosing this option returns a list of phones based on the specified lsc issued by search criteria.
d) **LSC Issuer Expires by** - Choosing this option returns a list of phones based on the specified lsc issuer expires by search criteria.
e) **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.

Generate 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 Communications Manager Administration, choose **Device** > **Phone**.

The **Find/List** window displays. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 13.

To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, choose a search pattern.

c) 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 3 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 4 In the Related Links drop-down list box, choose **CAPF Report in File**; then, click **Go**.

Step 5 Save the file to a location that you will remember.

Step 6 Use Microsoft Excel to open the.csv file.

Enter Phone Authentication String

If you chose the By Authentication String mode and generated an authentication string, you must enter the authentication string on the phone to install the locally significant certificate.

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.

Before you begin

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.
- The first node functions and runs. Ensure that the server runs for each certificate installation.
- The device has registered.
- A signed image exists on the phone; refer to the Cisco IP Phone Administration Guide.

Procedure

Step 1 Press the **Applications** button on the phone.

Step 2 If the configuration is locked, press ****#** (asterisk, asterisk, pound sign) to unlock it.

Step 3 Scroll down the **Settings** menu. Highlight “Security Configuration” and press the **Select** softkey.

Step 4 Scroll down the **Security Configuration** menu. Highlight “LSC” and press the **Update** softkey.

Step 5 When prompted for the authentication string, enter the string that the system provides and press the **Submit** softkey.

The phone installs, updates, deletes, or fetches the certificate, depending on the current CAPF configuration.

You can monitor the progress of the certificate operation by viewing the messages that display on the phone. After you press **Submit**, the message "Pending" displays under the LSC option. The phone generates the public and private key pair and displays the information on the phone. When the phone successfully completes the process, the phone displays a successful message. If the phone displays a failure message, you entered the wrong authentication string or did not enable the phone for upgrade.

You can stop the process by choosing the Stop option at any time.

Verify Phone Authentication String

You can verify that the certificate is installed on the phone by pressing the **Applications** button and selecting the **Model Information** menu.