Certificate Authority Proxy Function

Certificates Authority Proxy Function Overview

The Certificate Authority Proxy Function (CAPF) issues Locally Significant Certificates (LSCs) and authenticates endpoints.

The CAPF service runs on Unified Communications Manager and performs the following tasks:

- Issues LSCs to supported Cisco Unified IP Phones.

- Authenticates phones while in mixed mode.

- Upgrades existing LSCs for phones.

- Retrieves phone certificates for viewing and troubleshooting.

CAPF Service Certificate

The CAPF service gets automatically installed with the Unified Communications Manager installation and a CAPF-specific system certificate gets generated.

☞

Important   The following note is applicable only from Release 14SU2 onwards.

✎

| Note | For any CAPF certificates, it should include the following default X509 extensions: |

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

In the CAPF certificates if these extensions are missing, there will be TLS connection failure.

You can configure CAPF to operate in the following modes:

Table 1: CAPF Running Modes

Modes	Description
Cisco Authority Proxy Function	By default, the CAPF service on Unified Communications Manager issues CAPF service signed LSCs.
Online CA	Use this option to have an external online CA signed LSC for phones. The CAPF service connects automatically to the external CA. When a Certificate Signing Request (CSR) is manually submitted, the CA signs and returns the CA-signed LSC automatically.
Offline CA	Use this option if you want to use an offline external CA to sign LSC for phones. Manually download the LSC, submit them to the CA, and then upload the CA-signed certificates after they are ready. **Note** We recommend **Online CA** option instead of **Offline CA** when you want to use a third-party CA to sign LSC. **Online CA** is automated, quicker, and less likely to encounter problems.

Before you generate LSCs, make sure that you have the following:

- Unified Communications Manager Release 12.5 or later.

- Endpoints that use CAPF for certificates (includes Cisco Unified IP Phones and Jabber).

- Microsoft Windows Server 2012 and 2016 with CA configured.

- Domain Name Service (DNS).

As a pre-requisite, also decide how you want to authenticate your phones.

Upload CA root and HTTPS certificates before generating LSCs to the required trust stores. The Internet Information Services (IIS) hosts the HTTPS certificate. During a secure SIP connection, HTTPS certificate goes through the CAPF-trust and the CA root certificate goes through both the CAPF-trust and the Unified Communications Manager-trust. The CA root certificate is used to sign the Certificate Signing Requests (CSRs).

Following are the scenarios to upload the various certificates:

Table 2: Upload Certificate Scenarios

Scenarios	Actions
CA root and HTTPS certificates are same.	Upload the CA root certificate.
CA root and HTTPS certificates are different and the same CA root certificate issues the HTTPS certificates.	Upload the CA root certificate.
CA root certificate issues the intermediate CA and HTTPS certificates which are different.	Upload the CA root certificate.
The same CA root certificate issues CA root and HTTPS certificates which are different.	Upload CA root and HTTPS certificate.

Note We recommend using CAPF during a scheduled maintenance window as generating multiple certificates simultaneously may cause call-processing interruptions.

Certificates Authority Proxy Function Configuration Task Flow

Complete these tasks to configure the Certificate Authority Proxy Function (CAPF) service to issue LSCs for endpoints:

Note You don't have to restart the CAPF service after regenerating or uploading the new CAPF certificate.

Procedure

	Command or Action	Purpose
Step 1	Upload Root Certificate for Third-Party CAs	If you want your LSCs to be third-party CA-signed, upload the CA root certificate chain to the CAPF-trust store. Otherwise, you can skip this task.
Step 2	Upload Certificate Authority (CA) Root Certificate , on page 5	Upload the CA root certificate to the Unified Communications Manager Trust store.

	Command or Action	**Purpose**
Step 3	Configure Online Certificate Authority Settings, on page 5	Use this procedure to generate phone LSC certificates.
Step 4	Configure Offline Certificate Authority Settings	Use this procedure to generate phone LSC certificates using an Offline CA.
Step 5	Activate or Restart CAPF Services	After you configure the CAPF system settings, activate essential CAPF services.
Step 6	Configure CAPF settings in Unified Communications Manager using one of the following procedures: • Configure CAPF Settings in a Universal Device Template, on page 8 • Update CAPF Settings via Bulk Admin, on page 9 • Configure CAPF Settings for a Phone, on page 10	Add the CAPF settings to Phone Configuration using one of the following options: • If you haven't synced your LDAP directory, add CAPF settings to a Universal Device Template and apply settings through the initial LDAP sync. • Use Bulk Administration Tool to apply CAPF settings to many phones in a single operation. • You can apply CAPF settings on a phone-by-phone basis.
Step 7	Set KeepAlive Timer, on page 11	Set a keepalive value for the CAPF-Endpoint connection so that it's not timed out by a firewall. The default value is 15 minutes.

Upload Root Certificate for Third-Party CAs

Upload the CA root certificate to the CAPF-trust store and the Unified Communications Manager trust store to use an external CA to sign LSC certificates.

Note Skip this task if you don't want to use a third-party CA to sign LSCs.

Procedure

Step 1 From Cisco Unified OS Administration choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, choose **CAPF-trust**.

Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.

Step 5 Click **Browse**, navigate to the file, and then click **Open**.

Step 6 Click **Upload**.

Step 7   Repeat this task, uploading certificates to **callmanager-trust** for the **Certificate Purpose**.

Upload Certificate Authority (CA) Root Certificate

Note   Ensure that the intermediate or root CA certificate doesn't contain the 'CAPF−' substring in the Common Name. The 'CAPF−' common name is reserved for CAPF certificates.

Procedure

Step 1   From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2   Click **Upload Certificate/Certificate chain**.

Step 3   From the **Certificate Purpose** drop-down list, choose **callmanager-trust**.

Step 4   Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.

Step 5   Click **Browse**, navigate to the file, and then click **Open**.

Step 6   Click **Upload**.

Important   This Note is applicable from Release 14 SU2 onwards.

Note   For any root or intermediate CA certificates, it should include the following default X509 extensions:

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

In the certificates if these extensions are missing, there will be TLS connection failure.

Important   This Note is applicable from Release 14 SU3 onwards and only for IPSec certificates.

Note   For any CA-signed IPSec certificates, it should not include the following extensions:

X509v3 Basic Constraints:

CA:TRUE

Configure Online Certificate Authority Settings

Use this procedure in Unified Communications Manager to generate phone LSCs using Online CAPF.

Procedure

Step 1	From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
Step 2	From the **Server** drop-down list, choose a node where you activated the Cisco Certificate Authority Proxy Function (Active) service.
Step 3	From the **Service** drop-down list, choose **Cisco Certificate Authority Proxy Function (Active)**. Verify that the word "Active" is displayed next to the service name.
Step 4	From the **Certificate Issuer to Endpoint** drop-down list, choose **Online CA**. For CA-signed certificates, we recommend using an Online CA.
Step 5	In the **Duration Of Certificate Validity (in days)** field, enter a number between 1 and 1825 to represent the number of days that a certificate issued by CAPF is valid.
Step 6	In the **Online CA Parameters** section, set the following parameters in order to create the connection to the Online CA section.

- Online CA Hostname—The subject name or the Common Name (CN) should be the same as the Fully Qualified Domain Name (FQDN) of HTTPS certificate.

  Note   The hostname configured is the same as the Common Names (CN) of the HTTPs certificate hosted by Internet Information Services (IIS) running on Microsoft CA.

- Online CA Port—Enter the port number for Online CA. For example, 443

- Online CA Template—Enter the name of the template. Microsoft CA creates the template.

  Note   This field is enabled only if the Online CA Type is Microsoft CA.

- Online CA Type—Choose Microsoft CA or EST Supported CA for automatic enrollment of endpoint certificate.

  - Microsoft CA—Use this option when CA is Microsoft CA to allocate digital certificates to devices.

    Note   FIPS enabled mode is not supported with Microsoft CA.

  - **Important**   Supported from Release 14SU2 onwards.

    EST Supported CA—Use this option when CA supports inbuilt EST server mode for automatic enrollment.

- Online CA Username—Enter the username of the CA server.

- Online CA Password—Enter the password for the username of the CA server.

- Certificate Enrollment Profile Label—Enter the Digital Identity for EST Supported CA with valid characters.

  Note   This field is enabled only if the Online CA Type is EST Supported CA.

Step 7	Complete the remaining CAPF service parameters. Click the parameter name to view the service parameter help system.
Step 8	Click **Save**.

Step 9   Restart **Cisco Certificate Authority Proxy Function** for the changes to take effect. It automatically restarts the Cisco Certificate Enrollment service.

Current Online CA limitations

- The Online CA feature does not work if the CA server uses any other language apart from English. The CA server should respond only in English.

- The Online CA feature does not support mTLS authentication with CA.

- While using Online CA for LSC operation if LSC certificate is not provided with 'Digital signature' and 'key encipherment' key usage Device secure registration will fail.

- Device secure registration fails if LSC certificate is not provided with 'Digital signature' and 'key encipherment' while using Online CA for LSC operation.

Configure Offline Certificate Authority Settings

Follow this high-level process if you decide to generate phone LSC certificates using an Offline CA.

> **Note**   The offline CA option is more time-consuming than online CAs, involving numerous manual steps. Restart the process if there are any issues (for example, a network outage or phone reset) during the certificate generation and transmission process.

Procedure

Step 1   Download the root certificate chain from the third-party certificate authority.

Step 2   Upload the root certificate chain to the required trusts (CallManager trust CAPF trust) in Unified Communications Manager.

Step 3   Configure Unified Communications Manager to use Offline CAs by setting the **Certificate Issue to Endpoint** service parameter to Offline CA.

Step 4   Generate **CSR**s for your phone LSCs.

Step 5   Send the **CSR**s to the certificate authority.

Step 6   Obtain the signed certificates from the **CSR**.

For more detailed example on how to generate phone LSCs using an Offline CA, see CUCM Third-Party CA-Signed LSCs Generation and Import Configuration.

Activate or Restart CAPF Services

Activate the essential CAPF services after you configure the CAPF system settings. Restart if the CAPF service is already activated.

Procedure

Step 1	From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.
Step 2	From the **Server** drop-down list, select the publisher node and click **Go**.
Step 3	From the **Security Services** pane, check the services that apply:

- **Cisco Certificate Enrollment Service**—Check this service if you're using an Online CA else leave it unchecked.
- **Cisco Certificate Authority Proxy Function**—Check this service if unchecked (Deactivated). Restart if the service is already activated.

Step 4	Click **Save** if you modified any settings.
Step 5	If the **Cisco Certificate Authority Proxy Function** service was already checked (Activated), restart it:

    a) From the **Related Links** drop-down list, select **Control Center - Feature Services** and click **Go**.

    b) From **Security Settings** pane, check the **Cisco Certificate Authority Proxy Function** service and click **Restart**.

Step 6	Complete one of the following procedures to configure CAPF settings against individual phones.

Configure CAPF Settings in a Universal Device Template

Use this procedure to configure CAPF settings to a Universal Device Template. Apply the template against an LDAP directory sync through the feature group template configuration. The CAPF settings in the template apply to all synced devices that use this template.

Note You can only add the Universal Device Template to an LDAP directory that hasn't been synced. If your initial LDAP sync has occurred, use Bulk Administration to update phones. For details, see Update CAPF Settings via Bulk Admin, on page 9.

Procedure

Step 1	From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.
Step 2	Do either of the following:

- Click **Find** and **Select** an existing template.
- Click **Add New**.

Step 3	Expand the **Certificate Authority Proxy Function (CAPF) Settings** area.
Step 4	From the **Certificate Operation** drop-down list, select **Install/Upgrade**.
Step 5	From the **Authentication Mode** drop-down list menu, select an option for the device to authenticate itself.

Step 6   If you chose to use an authentication string, enter the **Authentication String** in the text box, or click **Generate String** to have the system generate a string for you.

Note	Authentication fails if this string isn't configured on the device itself.

Step 7   From the remaining fields, configure the key information. For help with the fields, see the online help.

Step 8   Click **Save**.

Note	Make sure you have configured the devices that use this template with the same authentication method that you assigned in this procedure. Otherwise, device authentication fails. See your phone documentation for details on how to configure authentication for phones.

Step 9   Apply the template settings to devices that use this profile.

   a)   Add the Universal Device Template to a Feature Group Template Configuration.
   b)   Add the Feature Group Template to an LDAP Directory Configuration that isn't synced.
   c)   Complete an LDAP sync. The CAPF settings get applied to all synced devices.

For details on configuring feature group templates and LDAP directories, see the "Configure End Users" section of System Configuration Guide for Cisco Unified Communications Manager.

Update CAPF Settings via Bulk Admin

Use **Update Phones** query of Bulk Administration to configure CAPF settings and LSC certificates for many existing phones in a single operation.

Note	If you haven't provisioned the phones, use **Insert Phones** menu of the Bulk Administration to provision new phones with CAPF settings from a CSV file. See the "Phones Insertions" section of Bulk Administration Guide for Cisco Unified Communications Manager for details on how to insert phones from CSV files.

Make sure you have configured your phones with the same string and authentication method that you plan to add in this procedure. Else, your phones don't authenticate to CAPF. See your *Phone Documentation* for details on how to configure authentication on the phone.

Procedure

Step 1   From Cisco Unified CM Administration, choose **Bulk Administration** > **Phones** > **Update Phones** > **Query**.

Step 2   Use filter options to limit the search to the phones that you want to update and click **Find**.

For example, use **Find phones where** drop-down list to select all phones, where LSC expires before a specific date or in a specific Device Pool.

Step 3   Click **Next**.

Step 4   From the **Logout/Reset/Restart** section, choose the **Apply Config** radio button. When the job runs, the CAPF updates get applied to all updated phones.

Step 5   Under **Certification Authority Proxy Function (CAPF) Information**, check the **Certificate Operation** check box.

Step 6	From the **Certificate Operation** drop-down list, choose **Install/Upgrade** to have CAPF install a new LSC certificate on the phone.
Step 7	From the **Authentication Mode** drop-down list, choose how you want the phone to authenticate itself during the LSC installation.

> **Note** Configure the same authentication method on the phone.

Step 8	Complete one of the following steps if you selected **By Authentication String** as the **Authentication Mode**:

- Check **Generate unique authentication string for each device** if you want to use a unique authentication string for each device.
- Enter the string in **Authentication String** text box, or click **Generate String** if you want to use the same authentication string for all devices.

Step 9	Complete the remaining fields in the **Certification Authority Proxy Function (CAPF) Information** section of the **Update Phones** window. For help with the fields and their settings, see the online help.
Step 10	From the **Job Information** section, select **Run Immediately**.

> **Note** Select **Run Later** if you want run the job at a scheduled time. For details on scheduling jobs, see the "Manage Scheduled Jobs" section in Bulk Administration Guide for Cisco Unified Communications Manager.

Step 11	Click **Submit**.

> **Note** Apply configurations in the **Phones Configuration** window for all updated phones if you didn't select the **Apply Config** option in this procedure.

Configure CAPF Settings for a Phone

Use this procedure to configure CAPF settings for LSC certificates on an individual phone.

> **Note** Use Bulk Administration or sync LDAP directory to apply CAPF settings to a large number of phones.

Configure your phone with the same string and authentication method that you plan to add in this procedure. Else, the phone doesn't authenticate itself to CAPF. See your *Phone Documentation* for details on how to configure authentication on the phone.

Procedure

Step 1	From Cisco Unified CM Administration, choose **Device** > **Phone**.
Step 2	Click **Find** and select an existing phone. The **Phone Configuration** page appears.
Step 3	Navigate to the **Certification Authority Proxy Function (CAPF) Information** pane.
Step 4	From the **Certificate Operation** drop-down list, choose **Install/Upgrade** for CAPF to install a new LSC certificate on the phone.

Step 5   From the **Authentication Mode** drop-down list, choose how you want the phone to authenticate itself during the LSC installation.

        Note   The phone should be configured to use the same authentication method.

Step 6   Enter a text string or click **Generate String** to generate a string for you if you selected **By Authentication String**.

Step 7   Enter the details in the remaining fields in the **Certification Authority Proxy Function (CAPF) Information** pane of the **Phone Configuration** page. For help with the fields and their settings, see the online help.

Step 8   Click **Save**.

Set KeepAlive Timer

Use this procedure to set the clusterwide keepalive timer for the CAPF–Endpoint connection so that the connection doesn't get timed out by a firewall. The timer has a default value of 15 minutes. After each interval, the CAPF service sends a keepalive signal to the phone to keep the connection open.

Procedure

Step 1   Use the Command Line Interface to login to the publisher node.

Step 2   Run the `utils capt set keep_alive` CLI command.

Step 3   Enter a number between 5 and 60 (minutes) and click **Enter**.

Certificates Authority Proxy Function Administration Task Flow

Administer LSC certificates on an ongoing basis once the CAPF is configured andcLSC certificates are issued.

Procedure

	Command or Action	Purpose
Step 1	LSC Generation via CAPF	Configure CAPF and add the configured authentication string on the phone. The keys and certificate exchange occurs between the phone and CAPF.
Step 2	Run Stale LSC Report	Run a Stale LSC report from Cisco Unified Reporting. Stale LSCs are certificates that were generated in response to an endpoint CSR, but were never installed because a new CSR was generated by the endpoint before the old LSC was installed.
Step 3	View Pending CSR List	View a list of pending CAPF CSR files. All CSR files are timestamped.

	Command or Action	**Purpose**
Step 4	Delete Stale LSC Certificates	Delete stale LSC certificates from the system.

Run Stale LSC Report

Use this procedure to run a Stale LSC report from Cisco Unified Reporting. Stale LSCs are certificates that were generated in response to an endpoint CSR, but were never installed because a new CSR was generated by the endpoint before the stale LSC was installed.

Note   You can also obtain a list of stale LSC certificates by running the `utils capf stale-lsc list` CLI command on the publisher node.

Procedure

Step 1	From Cisco Unified Reporting, choose **System Reports**.
Step 2	In the left navigation bar, choose **Stale LSCs**.
Step 3	Click **Generate a new report**.

LSC Generation via CAPF

After you configure CAPF, add the configured authentication string on the phone. The keys and certificate exchange occurs between the phone and CAPF and the following occurs:

- The phone authenticates itself to CAPF using the configured authentication method.

- The phone generates its public-private key pair.

- The phone forwards its public key to CAPF in a signed message.

- The private key remains in the phone and never gets exposed externally.

- CAPF signs the phone certificate and sends the certificate to the phone in a signed message.

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

Note   Key generation set at low priority allows the phone to function while the action occurs. 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

View Pending CSR List

Use this procedure to view a list of pending CAPF CSR files. All CSR files are timestamped.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capf csr list` CLI command.
A timestamped list of pending CSR files displays.

Delete Stale LSC Certificates

Use this procedure to delete stale LSC certificates from the system.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capf stale-lsc delete all` CLI command
The system deletes all stale LSC certificates from the system.

CAPF System Interactions

Table 3: CAPF System Interactions

Feature	Interaction
Authentication String	Enter the same authentication string on the phone after the operation in CAPF authentication method else the operation fails. The phone may fail and not recover until the matching authentication string is entered on the phone if TFTP Encrypted Configuration enterprise parameter is enabled and you fail to enter the authentication string.
Cluster Server Credentials	All servers in the Unified Communications Manager cluster must use the same administrator username and password, so CAPF can authenticate all servers in the cluster

Feature	Interaction
Migrating secure phone	If a secure phone gets moved to another cluster, the Unified Communications Manager doesn't trust the LSC certificate sent by the phone because it was issued by another CAPF, whose certificate isn't in the CTL file.
	Delete the existing CTL file to enable the secure phone to register. You can then use the Install/Upgrade option to install a new LSC certificate with a 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.
Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series	We recommend upgrading Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series to use LSCs for TLS connection to Unified Communications Manager and removing MIC root certificates from the Unified Communications Manager trust store to avoid possible future compatibility issues. Some phone models that use MICs for TLS connection to Unified Communications Manager may not be able to register.
	Administrators should remove the following MIC root certificates from the Unified Communications Manager trust store:
	• CAP-RTP-001
	• CAP-RTP-002
	• Cisco_Manufacturing_CA
	• Cisco_Root_CA_2048
Power Failures	The following information applies when a communication or power failure occurs.
	• The phone attempts to obtain the certificate three times in 30-second intervals if a communication failure occurs while installing the certificate on the phone. You can't configure these values.
	• If there's a power failure while the phone attempts a session with CAPF, the phone uses authentication mode stored in flash. System clears the flash value if the phone can't load a new configuration file from the TFTP server.
Certificate Encryption	Beginning from Unified Communications Manager Release 11.5(1) SU1, SHA-256 algorithm signs all the LSC certificates issued by CAPF service. Therefore, IP Phones 7900/8900/9900 series models supports SHA-256 signed LSC certicates and external SHA2 identity certificates (Tomcat, Unified Communications Manager, CAPF, TVS, and so on). Only SHA-1 supports any other cryptographic operation that requires validation of signature.
	Note We recommend using the Unified Communications Manager before 11.5(1) SU1 release for phone models in End of Software Maintenance or End of Life,

CAPF Examples with 7942 and 7962 Phones

Consider how CAPF interacts with the Cisco Unified IP Phone 7962 and 7942 when a user or Unified Communications Manager resets the phone.

Note   In the examples, CAPF certificate operation fails if LSC doesn't exist in the phone and you choose **By Existing Certificate** for the CAPF Authentication Mode.

Example-Nonsecure Device Security Mode

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 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 downloaded LSC, configure the Device Security Mode to Authenticated or Encrypted.

Example-Authenticated/Encrypted Device Security Mode

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 doesn't register with the primary 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 can't configure **By Authentication String** in this example because the phone doesn't automatically contact the CAPF server. The registration fails if the phone doesn't have a valid LSC.

CAPF Interaction with IPv6 Addressing

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

CAPF uses configurations from **Enable IPv6** enterprise parameter to issue or upgrade the certificate to the phone. If the enterprise parameter is **False**, CAPF ignores/rejects connections from phones that use IPv6 addresses, and the phone doesn't receive the certificate.

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

Table 4: 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 can't connect through an IPv6 address, it attempts to connect by using an IPv4 address.

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
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 can't connect to CAPF.
Two stack	IPv6	IPv4	Phone can't 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 stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4 stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4 stack	IPv4	IPv6	Phone can't connect to CAPF.
IPv6 stack	IPv6	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
IPv6 stack	IPv6	IPv4	Phone can't connect to CAPF.