



Cisco IP Conference Phone Security

- [Cisco IP Phone Security Overview, on page 1](#)
- [Security Enhancements for Your Phone Network, on page 2](#)
- [Supported Security Features, on page 3](#)
- [View the Current Security Features on the Phone, on page 9](#)
- [View Security Profiles, on page 10](#)
- [Configure the Security Settings, on page 10](#)

Cisco IP Phone Security Overview

The Security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and ensure that the phone uses only digitally signed files.

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for Cisco IP Phones without running the CTL client:

- Signing of the phone configuration files
- Phone configuration file encryption
- HTTPS with Tomcat and other Web services



Note Secure signaling and media features still require you to run the CTL client and use hardware eTokens.

For more information about the security features, see the documentation for your particular Cisco Unified Communications Manager release.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

A LSC cannot be used as the user certificate for EAP-TLS with WLAN authentication.

Alternatively, you can initiate the installation of an LSC from the Security Setup menu on the phone. This menu also lets you update or remove an LSC.

The Cisco IP Conference Phone 7832 complies with Federal Information Processing Standard (FIPS). To function correctly, FIPS mode requires an RSA key size of 2048 bits or greater. If the RSA server certificate is not 2048 bits or greater, the phone will not register with Cisco Unified Communications Manager and Phone failed to register. Cert key size is not FIPS compliant displays on the phone.

You cannot use private keys (LSC or MIC) in FIPS mode.

If the phone has an existing LSC that is smaller than 2048 bits, you need to update the LSC key size to 2048 bits or greater before enabling FIPS.

Related Topics

- [Set Up a Locally Significant Certificate](#), on page 11
- [Cisco Unified Communications Manager Documentation](#)

Security Enhancements for Your Phone Network

You can enable Cisco Unified Communications Manager 11.5(1) or later version to operate in an enhanced security environment. With these enhancements, your phone network operates under a set of strict security and risk management controls to protect you and your users.

The enhanced security environment includes the following features:

- Contact search authentication.
- TCP as the default protocol for remote audit logging.
- FIPS mode.
- An improved credentials policy.
- Support for the SHA-2 family of hashes for digital signatures.
- Support for a RSA key size of 512 and 4096 bits.



Note Your Cisco IP Phone can only store a limited number of Identity Trust List (ITL) files. ITL files cannot exceed 64K limit on phone so limit the number of files that the Cisco Unified Communications Manager sends to the phone.

SIP OAuth Support

SIP OAuth mode allows you to use OAuth refresh tokens for phone authentication.

Cisco Unified Communications Manager (Unified CM) verifies the token presented by the phone and serves the configuration files only to authorized ones. OAuth token validation during SIP registration is completed when OAuth-based authorization is enabled on Unified CM cluster and Cisco IP phones.

Cisco IP phones support SIP OAuth authentication on Proxy Trivial File Transfer Protocol (TFTP) and Cisco Unified Survivable Remote Site Telephony (SRST).

- SIP OAuth on TFTP requirements:
 - Cisco Unified Communications Manager Release 14.0(1)SU1 or later

- Cisco IP Phone Firmware Release 14.1(1) or later



Note Proxy TFTP and OAuth for Proxy TFTP aren't supported on Mobile Remote Access (MRA).

- SIP OAuth on SRST requirements:
 - Cisco Unified Communications Manager 14.0(1)SU1 or later
 - Cisco IP Phone Firmware Release 14.2(1) or later
 - Cisco SRST Software Release: IOS XE 17.8.1a or later
 - Cisco SRST Hardware Models: ISR1100, ISR43xx, ISR44xx, Catalyst 8200, or Catalyst 8300 platform

For information about how to configure SIP OAuth, see [SIP OAuth Mode in Security Guide for Cisco Unified Communications Manager](#).

Where to Find More Information about Phone Security

For additional information about security, see the following:

- *Security Guide for Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/14SU2/cucm_b_security-guide-14su2.html)
- *Cisco Unified SCCP and SIP SRST System Administration Guide* (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide/srst_roadmap.html)
- *System Configuration Guide for Cisco Unified Communications Manager*, Release 14.0(1) or later (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>).

Supported Security Features

Security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and ensure that the phone uses only digitally signed files.

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for Cisco IP Phones without running the CTL client:

- Signing of the phone configuration files
- Phone configuration file encryption
- HTTPS with Tomcat and other Web services



Note Secure signaling and media features still require you to run the CTL client and use hardware eTokens.

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains secure (encrypted) communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco IP Phones.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the Cisco Unified Communications Manager Security Guide. Alternatively, you can initiate the installation of an LSC from the Security Setup menu on the phone. This menu also lets you update or remove an LSC.

A LSC cannot be used as the user certificate for EAP-TLS with WLAN authentication.

The phones use the phone security profile, which defines whether the device is nonsecure or secure. For information about applying the security profile to the phone, see the documentation for your particular Cisco Unified Communications Manager release.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file contains sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see the documentation for your particular Cisco Unified Communications Manager release.

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

The following table provides an overview of the security features that the Cisco IP Conference Phone 7832 supports. For more information about these features, Cisco Unified Communications Manager, and Cisco IP Phone security, see the documentation for your particular Cisco Unified Communications Manager release.

Table 1: Overview of Security Features

| Feature | Description |
|--|---|
| Image authentication | Signed binary files (with the extension .sbn) prevent tampering. An image causes a phone to fail the authentication process and reject the image. |
| Customer-site certificate installation | Each phone requires a unique certificate for device authentication. For device authentication security, you can specify in Cisco Unified Communications Manager Administration the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a certificate on the phone. |
| Device authentication | Occurs between the Cisco Unified Communications Manager server and the phone. Determines whether a secure connection between the phone and the server is created. Creates a secure signaling path between the entities by using Transport Layer Security (TLS) unless they can be authenticated by the Cisco Unified Communications Manager server. |

| Feature | Description |
|--|---|
| File authentication | Validates digitally signed files that the phone downloads. The phone checks the signature of the file after the file creation. Files that fail authentication are not processed. |
| Signaling Authentication | Uses the TLS protocol to validate that no tampering has occurred. |
| Manufacturing installed certificate | Each phone contains a unique manufacturing installed certificate. This certificate is a unique proof of identity for the phone, and allows Cisco Unified Communications Manager to verify the phone's identity. |
| Secure SRST reference | After you configure a SRST reference for security and then enable SRST on the phone in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone's configuration. The phone uses a TLS connection to interact with the SRST-enabled router. |
| Media encryption | Uses SRTP to ensure that the media streams between supported devices are encrypted. Includes creating a media primary key pair for the phone and the other device while the keys are in transport. |
| CAPF (Certificate Authority Proxy Function) | Implements parts of the certificate generation procedure through the phone. The CAPF handles the generation and certificate installation. The CAPF can be configured to act on behalf of the phone, or it can be configured to generate certificates for the phone. |
| Security profiles | Defines whether the phone is nonsecure, authenticated, or secure. |
| Encrypted configuration files | Lets you ensure the privacy of phone configuration files. |
| Optional disabling of the web server functionality for a phone | You can prevent access to a phone web page, which displays the phone's status and configuration. |
| Phone hardening | Additional security options, which you control from Cisco Unified Communications Manager Administration. <ul style="list-style-type: none"> • Disable access to web pages for a phone <p>Note You can view current settings for the GARP E menu.</p> |
| 802.1X Authentication | The phone can use 802.1X authentication to request and gain access to network resources. |


| Feature | Description |
|---|---|
| AES 256 Encryption | <p>When connected to Cisco Unified Communications Manager IP Phones, TLS and SIP for signaling and media encryption. This enables protocols that conform to SHA-2 (Secure Hash Algorithm) standards and the following ciphers are:</p> <ul style="list-style-type: none"> • For TLS connections: <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • For sRTP: <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM <p>For more information, see the Cisco Unified Communications Manager IP Phone Security Configuration Guide.</p> |
| Elliptic Curve Digital Signature Algorithm (ECDSA) certificates | As part of Common Criteria (CC) certification, Cisco Unified Communications Manager IP Phones support all Voice Operating System (VOS) products from version Cisco IOS 12.4(2)T. |

Related Topics

[Cisco Unified Communications Manager Documentation](#)

Phone Call Security

When security is implemented for a phone, you can identify secure phone calls by icons on the phone screen. You can also determine whether the connected phone is secure and protected if a security tone plays at the beginning of the call.

In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security, providing integrity and privacy to the call. When a call in progress is encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to the following icon: .



Note If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

In a secure call, a security tone plays at the beginning of a call to indicate that the other connected phone is also receiving and transmitting secure audio. If your call connects to a nonsecure phone, the security tone does not play.




Note Secure calling is supported between two phones. Secure conference, Cisco Extension Mobility, and shared lines can be configured by a secure conference bridge.

When a phone is configured as secure (encrypted and trusted) in Cisco Unified Communications Manager, it can be given a “protected” status. After that, if desired, the protected phone can be configured to play an indication tone at the beginning of a call:

- **Protected Device:** To change the status of a secure phone to protected, check the Protected Device check box in the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device > Phone**).
- **Play Secure Indication Tone:** To enable the protected phone to play a secure or nonsecure indication tone, set the Play Secure Indication Tone setting to True. By default, Play Secure Indication Tone is set to False. You set this option in Cisco Unified Communications Manager Administration (**System > Service Parameters**). Select the server and then the Unified Communications Manager service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. The default is False.

Secure Conference Call Identification

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established by using this process:

1. A user initiates the conference from a secure phone.
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays the secure icon  to the right of **Conference** on the phone screen.



Note Secure calling is supported between two phones. For protected phones, some features, such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured.

The following table provides information about changes to conference security levels depending on the initiator phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 2: Security Restrictions with Conference Calls


| Initiator Phone Security Level | Feature Used | Security Level of Participants | Results of Action |
|--------------------------------|--------------|-----------------------------------|---|
| Nonsecure | Conference | Secure | Nonsecure conference bridge Nonsecure conference |
| Secure | Conference | At least one member is nonsecure. | Secure conference bridge Nonsecure conference |
| Secure | Conference | Secure | Secure conference bridge Secure encrypted level conference |

| Initiator Phone Security Level | Feature Used | Security Level of Participants | Results of Action |
|--------------------------------|--------------|--------------------------------------|---|
| Nonsecure | Meet Me | Minimum security level is encrypted. | Initiator receives message Does not meet Security Level, call rejected. |
| Secure | Meet Me | Minimum security level is nonsecure. | Secure conference bridge Conference accepts all calls. |

Secure Phone Call Identification

A secure call is established when your phone, and the phone on the other end, is configured for secure calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Secured calls can only be made between two phones. Conference calls should support secure call after secure conference bridge set up.

A secured call is established using this process:

1. A user initiates the call from a secured phone (secured security mode).
2. The phone displays the secure icon  on the phone screen. This icon indicates that the phone is configured for secure calls, but this does not mean that the other connected phone is also secured.
3. The user hears a security tone if the call connects to another secured phone, indicating that both ends of the conversation are encrypted and secured. If the call connects to a nonsecure phone, the user does not hear the security tone.



Note Secure calling is supported between two phones. For protected phones, some features, such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured.

Only protected phones play these secure or nonsecure indication tones. Nonprotected phones never play tones. If the overall call status changes during the call, the indication tone changes and the protected phone plays the appropriate tone.

A protected phone plays a tone or not under these circumstances:

- When the Play Secure Indication Tone option is enabled:
 - When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone (three long beeps with pauses).
 - When end-to-end nonsecure media is established and the call status is nonsecure, the phone plays the nonsecure indicationtone (six short beeps with brief pauses).

If the Play Secure Indication Tone option is disabled, no tone plays.

802.1x Authentication

The Cisco IP Phones support 802.1X Authentication.

Cisco IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. Phones contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.
- Cisco Catalyst Switch (or other third-party switch): The switch must support 802.1X, so it can act as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure Voice VLAN—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
 - Enabled—If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
 - Disabled—If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

Related Topics

[Cisco Unified Communications Manager Documentation](#)

View the Current Security Features on the Phone

For more information about the security features and about Cisco Unified Communications Manager and Cisco IP Phone security, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

-
- Step 1** Select **Settings**.
- Step 2** Select **Admin Settings > Security Setup**.

Most security features are available only if a certificate trust list (CTL) is installed on the phone.

Related Topics

[Cisco Unified Communications Manager Documentation](#)

View Security Profiles

All Cisco IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

-
- Step 1** In Cisco Unified Communications Manager Administration, select **System > Security > Phone Security Profile**.
- Step 2** Look at the Security Mode setting.

Related Topics

[Cisco Unified Communications Manager Documentation](#)

Configure the Security Settings

Procedure

-
- Step 1** Press **Settings**.
- Step 2** Select **Admin Settings > Security Setup**.
- Step 3** Set the fields.
After you set the fields, you may need to reboot the phone.

Security Setup Fields

The Security Setup menu contains fields and submenus for trust lists and 802.1x authentication.

Table 3: Security Setup Menu

| Entry | Type | Default | Description |
|-----------------------|------|---------|--|
| Security mode | | | Read only |
| LSC | | | See Set Up a Locally Significant Certificate, on page 11 . |
| Trust List | Menu | | See the “Trust List Submenu” table. |
| 802.1x Authentication | Menu | | See the “802.1x Authentication Submenu” table. |

Table 4: Trust List Submenu

| Entry | Type | Default | Description |
|------------------------|------|---------|--|
| CTL File | Menu | | Displays a list of CTL files |
| ITL File | Menu | | Displays a list of ITL files |
| Configuration (signed) | Menu | | See the “Configuration Submenu table.” |

Table 5: Configuration Submenu

| Entry | Type | Default | Description |
|-------------|------|---------|----------------------------------|
| SRST Router | | | Displays the IP address of SRST. |

Table 6: 802.1x Authentication Submenu

| Entry | Type | Default | Description |
|-----------------------|---------------------|----------|---|
| Device authentication | Disabled Enabled | Disabled | |
| Transaction Status | Submenu | | See the “Transaction Status Submenu” table. |

Table 7: Transaction Status Submenu

| Entry | Type | Default | Description |
|--------------------|---------------------------|---------|--------------------|
| Transaction Status | Disconnected Connected | | |
| Protocols | | | List of protocols. |

Set Up a Locally Significant Certificate

This task applies to setting up a LSC with the authentication string method.

Before you begin

Make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL or ITL file has a CAPF certificate.
- In Cisco Unified Communications Operating System Administration, verify that the CAPF certificate is installed.
- The CAPF is running and configured.

For more information about these settings, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

Step 1 Obtain the CAPF authentication code that was set when the CAPF was configured.

Step 2 From the phone, press **Applications** .

Step 3 From the phone, choose **Settings**.

Step 4 Choose **Admin Settings > Security Setup**.

Note You can control access to the Settings menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window.

Step 5 Choose **LSC** and press **Select** or **Update**.

The phone prompts for an authentication string.

Step 6 Enter the authentication code and press **Submit**.

The phone begins to install, update, or remove the LSC, depending on how the CAPF is configured. During the procedure, a series of messages appears in the LSC option field in the Security Configuration menu, so you can monitor progress. When the procedure is complete, `Installed` or `Not Installed` displays on the phone.

The LSC install, update, or removal process can take a long time to complete.

When the phone installation procedure is successful, the `Installed` message displays. If the phone displays `Not Installed`, then the authorization string may be incorrect or the phone upgrade may not be enabled. If the CAPF operation deletes the LSC, the phone displays `Not Installed` to indicate that the operation succeeded. The CAPF server logs the error messages. See the CAPF server documentation to locate the logs and to understand the meaning of the error messages.

Related Topics

[Cisco Unified Communications Manager Documentation](#)

Enable FIPS Mode

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device > Phone** and locate the phone.

Step 2 Navigate to the Product Specific Configuration area.

Step 3 Set the **FIPS Mode** field to Enabled.

Step 4 Select **Apply Config**.

Step 5 Select **Save**.

Step 6 Restart the phone.
