



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](#)

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 8832 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 in the phone's status messages.

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 6
[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 8832 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. If an unsigned image causes a phone to fail the authentication process and reject the image, the phone will not load 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 established and 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.
File authentication	Validates digitally signed files that the phone downloads. The phone checks the signature after the file creation. Files that fail authentication are not written to the phone and are not processed.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred during the signaling process.

Feature	Description
Manufacturing installed certificate	Each phone contains a unique manufacturing installed certificate, which provides 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 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. The keys are in transport while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure through the phone's configuration. The CAPF can be configured to generate and install certificates 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 configuration.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager. <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.
AES 256 Encryption	When connected to Cisco Unified Communications Manager, the phone uses TLS and SIP for signaling and media encryption. This enables the phone to use ciphers that conform to SHA-2 (Secure Hash Algorithm) standards. The supported ciphers are: <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 Security Guide.</p>
Elliptic Curve Digital Signature Algorithm (ECDSA) certificates	As part of Common Criteria (CC) certification, Cisco Unified Communications Manager supports ECDSA certificates for all Voice Operating System (VOS) products from version 9.1(1) onwards.

Related Topics[Cisco Unified Communications Manager Documentation](#)

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, choose **Settings**.

Step 3 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 4 Choose **LSC** and press **Select** or **Update**.

The phone prompts for an authentication string.

Step 5 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. |
-

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
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.

Provide Encryption for Barge

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and security in the system.

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder (fast busy) tone plays on the phone that the barge was initiated.

If the initiator phone is configured for encryption, the barge initiator can barge into a nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

WLAN Security

Because all WLAN devices that are within range can receive all other WLAN traffic, securing voice communications is critical in WLANs. To ensure that intruders do not manipulate nor intercept voice traffic,

the Cisco SAFE Security architecture supports the Cisco IP Phone and Cisco Aironet APs. For more information about security in networks, see

http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications by using the following authentication methods that the wireless Cisco IP Phone supports:

- **Open Authentication:** Any wireless device can request authentication in an open system. The AP that receives the request may grant authentication to any requestor or only to requestors that are found on a list of users. Communication between the wireless device and AP could be nonencrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that use WEP only attempt to authenticate with an AP that is using WEP.
- **Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication:** This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server, such as the Cisco Access Control Server (ACS).

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with the primary key. Both endpoints now contain the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS server.



Note In the Cisco ACS, by default, the PAC expires in one week. If the phone has an expired PAC, authentication with the RADIUS server takes longer while the phone gets a new PAC. To avoid PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

- **Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) Authentication:** EAP-TLS requires a client certificate for authentication and network access. For wired EAP-TLS, the client certificate can be either the phone's MIC or an LSC. LSC is the recommended client authentication certificate for wired EAP-TLS.
- **Protected Extensible Authentication Protocol (PEAP):** Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco IP Phone can use PEAP for authentication with the wireless network. Only PEAP-MSCHAPV2 is supported. PEAP-GTC is not supported.

The following authentication schemes use the RADIUS server to manage authentication keys:

- **WPA/WPA2:** Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA preshared keys that are stored on the AP and phone.
- **Fast Secure Roaming:** Uses RADIUS server and a wireless domain server (WDS) information to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication. The Cisco IP Phone 8800 Series supports 802.11r (FT). Both 11r (FT) and CCKM are supported to allow for fast secure roaming. But Cisco strongly recommends to utilize the 802.11r (FT) over air method.

With WPA/WPA2 and CCKM, encryption keys are not entered on the phone, but are automatically derived between the AP and phone. But the EAP username and password that are used for authentication must be entered on each phone.

To ensure that voice traffic is secure, the Cisco IP Phone supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, both the signalling SIP packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the Cisco IP Phone.

WEP

With WEP use in the wireless network, authentication happens at the AP by using open or shared-key authentication. The WEP key that is setup on the phone must match the WEP key that is configured at the AP for successful connections. The Cisco IP Phone supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and AP.

EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the AP after authentication for encrypting all voice packets; consequently, these WEP keys can change with each authentication.

TKIP

WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.

AES

An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, which supports key sizes of 128, 192 and 256 bits, as a minimum. The Cisco IP Phone supports a key size of 256 bits.



Note The Cisco IP Phone does not support Cisco Key Integrity Protocol (CKIP) with CMIC.

Authentication and encryption schemes are set up within the wireless LAN. VLANs are configured in the network and on the APs and specify different combinations of authentication and encryption. An SSID associates with a VLAN and the particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the Cisco IP Phone.

Some authentication schemes require specific types of encryption. With Open authentication, you can use static WEP for encryption for added security. But if you are using Shared Key authentication, you must set static WEP for encryption, and you must configure a WEP key on the phone.



-
- Note**
- When you use WPA pre-shared key or WPA2 pre-shared key, the pre-shared key must be statically set on the phone. These keys must match the keys that are on the AP.
 - The Cisco IP Phone does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.
-

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the Cisco IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 3: Authentication and Encryption Schemes

Cisco IP Phone Configuration	AP Configuration			
	<u>Security</u>	<u>Key Management</u>	<u>Encryption</u>	<u>Fast Roaming</u>
None	None	None	None	N/A
WEP	Static WEP	Static	WEP	N/A
PSK	PSK	WPA	TKIP	None
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

For more information about configuring authentication and encryption schemes on APs, see the *Cisco Aironet Configuration Guide* for your model and release under the following URL:

<http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243>

Wireless LAN Security

Cisco phones that support Wi-Fi have more security requirements and require extra configuration. These extra steps include installing certificates and setting up security on the phones and on the Cisco Unified Communications Manager.

For additional information, see *Security Guide for Cisco Unified Communications Manager*.

Cisco IP Phone Administration Page

Cisco phones that support Wi-Fi have special web pages that are different from the pages for other phones. You use these special web pages for phone security configuration when Simple Certificate Enrollment Protocol

(SCEP) is not available. Use these pages to manually install security certificates on a phone, to download a security certificate, or to manually configure the phone date and time.

These web pages also show the same information that you see on other phone web pages, including device information, network setup, logs, and statistical information.

Configure the Administration Page for Phone

The administration web page is enabled when the phone ships from the factory and the password is set to Cisco. But if a phone registers with Cisco Unified Communications Manager, the administration web page must be enabled and a new password configured.

Enable this web page and set the sign-in credentials before you use the web page for the first time after the phone has registered.

Once enabled, the administration web page is accessible at HTTPS port 8443 (**`https://x.x.x.x:8443`**, where x.x.x.x is a phone IP address).

Before you begin

Decide on a password before you enable the administration web page. The password can be any combination of letters or numbers, but it must be between 8 and 127 characters in length.

Your username is permanently set to admin.

Procedure

-
- | | |
|---------------|---|
| Step 1 | From the Cisco Unified Communications Manager Administration, select Device > Phone . |
| Step 2 | Locate your phone. |
| Step 3 | In the Product Specific Configuration Layout section, set Web Admin to Enabled . |
| Step 4 | In the Admin Password field, enter a password. |
| Step 5 | Select Save and click OK . |
| Step 6 | Select Apply Config and click OK . |
| Step 7 | Restart the phone. |
-

Access the Phone Administration Web Page

When you want to access the administration web pages, you need to specify the administration port.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Obtain the IP address of the phone: <ul style="list-style-type: none">• In Cisco Unified Communications Manager Administration, select Device > Phone, and locate the phone. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window. |
| Step 2 | Open a web browser and enter the following URL, where <i>IP_address</i> is the IP address of the Cisco IP Phone:
<code>https://<IP_address>:8443</code> |

- Step 3** Enter the password in the Password field.
- Step 4** Click **Submit**.
-

Install a User Certificate from the Phone Administration Web Page

You can manually install a user certificate on the phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

The preinstalled Manufacturing Installed Certificate (MIC) can be used as the User Certificate for EAP-TLS. After the User Certificate installs, you need to add it to the RADIUS server trust list.

Before you begin

Before you can install a User Certificate for a phone, you must have:

- A User Certificate saved on your PC. The certificate must be in PKCS #12 format.
- The certificate's extract password.

Procedure

- Step 1** From the phone administration web page, select **Certificates**.
- Step 2** Browse to the certificate on your PC.
- Step 3** In the **Extract password** field, enter the certificate extract password.
- Step 4** Click **Upload**.
- Step 5** Restart the phone after the upload is complete.
-

Install an Authentication Server Certificate from the Phone Administration Web Page

You can manually install an Authentication Server certificate on the phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

The root CA certificate that issued the RADIUS server certificate must be installed for EAP-TLS.

Before you begin

Before you can install a certificate on a phone, you must have an Authentication Server Certificate saved on your PC. The certificate must be encoded in PEM (Base-64) or DER.

Procedure

- Step 1** From the phone administration web page, select **Certificates**.
- Step 2** Locate the **Authentication server CA (Admin webpage)** field and click **Install**.
- Step 3** Browse to the certificate on your PC.
- Step 4** Click **Upload**.
- Step 5** Restart the phone after the upload is complete.

If you are installing more than one certificate, install all of the certificates before restarting the phone.

Manually Remove a Security Certificate from the Phone Administration Web Page

You can manually remove a security certificate from a phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

Procedure

- Step 1** From the phone administration web page, select **Certificates**.
 - Step 2** Locate the certificate on the **Certificates** page.
 - Step 3** Click **Delete**.
 - Step 4** Restart the phone after the deletion process completes.
-

Manually Set the Phone Date and Time

With certificate-based authentication, the phone must display the correct date and time. An authentication server checks the phone date and time against the certificate expiry date. If the phone and the server dates and times don't match, the phone stops working.

Use this procedure to manually set the date and time on the phone if the phone is not receiving the correct information from your network.

Procedure

- Step 1** From the phone administration web page, scroll to **Date & Time**.
 - Step 2** Perform one of the following options:
 - Click **Set Phone to Local Date & Time** to synch the phone to a local server.
 - In the **Specify Date & Time** fields, select the month, day, year, hour, minute, and second using the menus and click **Set Phone to Specific Date & Time**.
-

SCEP Setup

Simple Certificate Enrollment Protocol (SCEP) is the standard for automatically provisioning and renewing certificates. It avoids manual installation of certificates on your phones.

Configure the SCEP Product Specific Configuration Parameters

You must configure the following SCEP parameters on your phone web page

- RA IP address
- SHA-1 or SHA-256 fingerprint of the root CA certificate for the SCEP server

The Cisco IOS Registration Authority (RA) serves as a proxy to the SCEP server. The SCEP client on the phone use the parameters that are downloaded from Cisco Unified Communication Manager. After you configure the parameters, the phone sends a SCEP `getcs` request to the RA and the root CA certificate is validated using the defined fingerprint.

Procedure

-
- Step 1** From the Cisco Unified Communications Manager Administration, select **Device > Phone**.
 - Step 2** Locate the phone.
 - Step 3** Scroll to the **Product Specific Configuration Layout** area.
 - Step 4** Check the **WLAN SCEP Server** check box to activate the SCEP parameter.
 - Step 5** Check the **WLAN Root CA Fingerprint (SHA256 or SHA1)** check box to activate the SCEP QED parameter.
-

Simple Certificate Enrollment Protocol Server Support

If you are using a Simple Certificate Enrollment Protocol (SCEP) server, the server can automatically maintain your user and server certificates. On the SCEP server, configure the SCEP Registration Agent (RA) to:

- Act as a PKI trust point
- Act as a PKI RA
- Perform device authentication using a RADIUS server

For more information, see your SCEP server documentation.

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](#)

