Phone Security Profile Setup

This chapter provides information about security profile setup.

Phone Security Profile Overview

Unified Communications Manager Administration groups security-related settings for a phone type and protocol into security profiles to allow you to assign a single security profile to multiple phones. Security-related settings include device security mode, digest authentication, and some CAPF settings. You apply the configured settings to a phone when you choose the security profile in the Phone Configuration window.

Installing Unified Communications Manager provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone.

Only the security features that the selected device and protocol support display in the security profile settings window.

Phone Security Profile Setup Prerequisites

Consider the following information before you configure the phone security profiles:

- When you configure phones, choose a security profile in the **Phone Configuration** window. If the device does not support security or a secure profile, apply a non-secure profile.
- You cannot delete or change the predefined non-secure profiles.
- You cannot delete a security profile that is currently assigned to a device.

- If you change the settings in a security profile that is already assigned to a phone, the re-configured settings apply to all phones that are assigned that particular profile.
- You can rename security files that are assigned to devices. The phones that are assigned with the earlier profile name and settings assume the new profile name and settings.
- The CAPF settings, the authentication mode and the key size, are displayed in the **Phone Configuration** window. You must configure CAPF settings for certificate operations that involve MICs or LSCs. You can update these fields directly in the **Phone Configuration** window.
  - If you update the CAPF settings in the security profile, the settings are also updated in the Phone Configuration window.
  - If you update the CAPF settings in the Phone Configuration window and a matching profile is found, Unified Communications Manager applies the matching profile to the phone.
  - If you update the CAPF settings in the Phone Configuration window, and no matching profiles are found, Unified Communications Manager creates a new profile and applies that profile to the phone.
- If you have configured the device security mode earlier to an upgrade, Unified Communications Manager creates a profile that is based on that model and protocol and applies the profile to the device.
- We recommend that you use MICs for LSC installation only. Cisco support LSCs to authenticate the TLS connection with Unified Communications Manager. Since MIC root certificates can be compromised, users who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.
- We recommend that you upgrade Cisco IP Phones to use LSCs for TLS connections and remove the MIC root certificates from the CallManager trust store to avoid compatibility issues.

Find Phone Security Profile

To find a phone security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

Records from an active (prior) query may also display in the window.

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

To filter or search records

a) From the first drop-down list, choose a search parameter.
b) From the second drop-down list, choose a search pattern.
c) Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 4 From the list of records that display, click the link for the record that you want to view.

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

The window displays the record that you choose.

Set Up Phone Security Profile

To setup a phone security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Security Profile > Phone Security Profile**.

Step 2 Perform one of the following tasks:

a) To add a new profile, click **Add New**.
b) To copy an existing security profile, locate the appropriate profile, click **Copy** next to the security profile that you want to copy, and continue.
c) To update an existing profile, locate the appropriate security profile and continue.

When you click **Add New**, the configuration window displays with the default settings for each field. When you click **Copy**, the configuration window displays the copied settings.

Step 3 Enter appropriate settings for phones that are running SCCP or SIP.

Step 4 Click **Save**.

Phone Security Profile Settings

The following table describes the settings for the security profile for the phone that is running SCCP.

Only settings that the selected phone type and protocol support display.

Table 1: Security Profile for Phone That Is Running SCCP

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **Device Security Profile** drop-down list in the **Phone Configuration window** for the phone type and protocol. **Tip** Include the device model and protocol in the security profile name to find the correct profile while searching for a profile or updating a profile.
Description	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Setting	Description
Device Security Mode	

Setting	Description
	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image, file, and device authentication exist for the phone. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and signalling encryption for the trunk. The following are the supported ciphers: **TLS Ciphers** This parameter defines the ciphers that are supported by the Unified Communications Manager for establishing SIP TLS and inbound CTI Manager TLS connections. Strongest- AES-256 SHA-384 only: RSA Preferred • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Strongest - AEAD AES-256 GCM cipher only'. With this option chosen, the phones will not register on authenticated mode. Strongest- AES-256 SHA-384 only: ECDSA Preferred • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` Medium- AES-256 AES-128 only: RSA Preferred **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Strongest - AEAD AES-256 GCM cipher only'. With this option chosen, the phones will not register on authenticated mode. • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256` • `TLS_ECDHE_ECDSA with AES128_GCM_SHA256` **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Medium - AEAD AES-256,AES-128 GCM ciphers only'. With this option chosen, the phones will not register on authenticated mode. Medium- AES-256 AES-128 only: ECDSA Preferred

Setting	Description
	• TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Medium - AEAD AES-256,AES-128 GCM ciphers only'. With this option chosen, the phones will not register on authenticated mode. All Ciphers, RSA Preferred: • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 All Ciphers, ECDSA Preferred: • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 **Note** If the trunks are configured with Device Security Profile option selected as Authenticated, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as Encrypted. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
TFTP Encrypted Config	When this check box is checked, Unified Communications Manager encrypts a phone downloads from the TFTP server.

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • **By Authentication String**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate without the user intervention. This option provides no security. We recommend that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If an LSC exists in the phone, authentication occurs through the LSC, regardless whether a MIC exists in the phone. If a MIC and an LSC exist in the phone, authentication occurs through the LSC. If an LSC does not exist in the phone, but a MIC exists, authentication occurs through the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF although a MIC and an LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate if an LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs through the MIC, regardless whether an LSC exists in the phone. If an LSC exists in the phone, but a MIC does not exist, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.

Setting	Description
Key Order	This field specifies the sequence of the key for CAPF. Select one of the following values from the drop-down list: • **RSA Only** • **EC Only** • **EC Preferred, RSA Backup** **Note** When you add a phone, that is based on the value in **Key Order**, **RSA Key Size**, and **EC Key Size** fields, the device security profile is associated with the phone. If you select the **EC Only** value, with the **EC Key Size** value of 256 bits, then the device security profile appends with **EC-256** value.
RSA Key Size (Bits)	From the drop-down list box, choose one of the values—**512**, **1024**, **2048, 3072**, or **4096**. **Note** Some phone models may fail to register if the RSA **key length** that is selected for the CallManager **Certificate Purpose** is greater than 2048. From the *Unified CM Phone Feature List Report* on the *Cisco Unified Reporting Tool (CURT)*, you can check the 3072/4096 RSA key size support feature for the list of supported phone models.
EC Key Size (Bits)	From the drop-down list, choose one of the values—**256**, **384**, or **521**.

The following table describes the settings for the security profile for the phone that is running SIP.

Table 2: Security Profile for Phone That Is Running SIP

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **Device Security Profile** drop-down list in the **Phone Configuration** window for the phone type and protocol. **Tip** Include the device model and protocol in the security profile name to help you find the correct profile when you are searching for or updating a profile.
Description	Enter a description for the security profile.
Nonce Validity Time	Enter the number of minutes (in seconds) that the nonce value is valid. The default value equals 600 (10 minutes). When the time expires, Unified Communications Manager generates a new value. **Note** A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.

Setting	Description
Device Security Mode	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image, file, and device authentication exist for the phone. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and encryption for the phone. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all phone calls on all SRTP-capable hops. **Note** If the trunks are configured with Device Security Profile option selected as Authenticated, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as Encrypted. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
Transport Type	When Device Security Mode is **Non Secure**, choose one of the following options from the drop-down list (some options may not display): • **TCP**—Choose the Transmission Control Protocol to ensure that packets get received in the same order as the order in which they are sent. This protocol ensures that no packets get dropped, but the protocol does not provide any security. • **UDP**—Choose the User Datagram Protocol to ensure that packets are received quickly. This protocol, which can drop packets, does not ensure that packets are received in the order in which they are sent. This protocol does not provide any security. • **TCP + UDP**—Choose this option if you want to use a combination of TCP and UDP. This option does not provide any security. When Device Security Mode is **Authenticated** or **Encrypted**, TLS specifies the Transport Type. TLS provides signaling integrity, device authentication, and signaling encryption (encrypted mode only) for SIPphones. If Device Security Mode cannot be configured in the profile, the transport type specifies UDP.

Setting	Description
Enable Digest Authentication	If you check this check box, Unified Communications Manager challenges all SIP requests from the phone. Digest authentication does not provide a device authentication, integrity, or confidentiality. Choose a security mode of authenticated or encrypted to use these features.
TFTP Encrypted Config	When this check box is checked, Unified Communications Manager encrypts the phone downloads from the TFTP server. This option exists for Cisco phones only. **Tip** We recommend that you enable this option and configure a symmetric key to secure digest credentials and administrative passwords.
Exclude Digest Credentials in Configuration File	When this check box is checked, Unified Communications Manager omits digest credentials in the phone downloads from the TFTP server. This option exists for Cisco IP Phones, 7942, and 7962 (SIP only).

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. This option exists for Cisco phones only. From the drop-down list, choose one of the following options: • **By Authentication String**—Installs or upgrades or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**—Installs or upgrades or troubleshoots a locally significant certificate without the user intervention. This option provides no security; we recommend that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**—Installs or upgrades or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If an LSC exists in the phone, authentication occurs through the LSC, regardless whether a MIC exists in the phone. If an LSC does not exist in the phone, but a MIC does exist, authentication occurs through the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF although a MIC and an LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs or upgrades or troubleshoots a locally significant certificate if an LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs through the MIC, regardless whether an LSC exists in the phone. If an LSC exists in the phone, but a MIC does not exist, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. The default setting equals 1024. The other option for key size is 512. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.
SIP Phone Port	This setting applies to phones that are running SIP that uses UDP transport. Enter the port number for Cisco Unified IP Phone (SIP only) that use UDP to listen for SIP messages from Unified Communications Manager. The default setting equals 5060. Phones that use TCP or TLS ignore this setting.

Apply Security Profiles to Phone

Before you apply a security profile that uses certificates for authentication of the phone, make sure that the particular phone contains a Locally Significant Certificate (LSC) or Manufacture-Installed Certificate (MIC).

To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. However, if the phone does not contain a certificate, perform the following tasks:

- In the **Phone Configuration** window, apply a non-secure profile.
- In the **Phone Configuration** window, install a certificate by configuring the CAPF settings.
- In the **Phone Configuration** window, apply a device security profile that is configured for authentication or encryption.

To apply a phone security profile to a device, perform the following procedure:

Procedure

Step 1 Go to the **Protocol Specific Information** section in the **Phone Configuration** window.

Step 2 From the **Device Security Profile** drop-down list, choose the security profile that applies to the device. The phone security profile that is configured only for the phone type and the protocol is displayed.

Step 3 Click **Save**.

Step 4 To apply the changes to the applicable phone, click **Apply Config**.

Note To delete security profiles, check the check boxes next to the appropriate security profile in the **Find and List** window, and click **Delete Selected**.

Synchronize Phone Security Profile with Phones

To synchronize phone security profile with phones, perform the following procedure:

Procedure

Step 1 From Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

Step 2 Choose the search criteria to use and click **Find**.
The window displays a list of phone security profiles that match the search criteria.

Step 3 Click the phone security profile to which you want to synchronize the applicable phones.

Step 4 Make any additional configuration changes.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.
The **Apply Configuration Information** dialog box appears.

Step 7 Click **OK**.

Delete Phone Security Profile

Before you can delete a security profile from Unified Communications Manager, you must apply a different profile to the devices or delete all devices that use the profile.

To find out which devices use the profile, perform Step 1:

Procedure

Step 1 In the **Security Profile Configuration** window, choose **Dependency Records** from the **Related Links** drop-down list and click **Go**.

If the dependency records feature is not enabled for the system, go to **System** > **Enterprise Parameters Configuration** and change the Enable Dependency Records setting to **True**. A message displays information about high CPU consumption that relates to the dependency records feature. Save your change to activate dependency records. For more information about dependency records, see System Configuration Guide for Cisco Unified Communications Manager

This section describes how to delete a phone security profile from the Unified Communications Manager database.

Step 2 Find the security profile to delete.

Step 3 To delete multiple security profiles, check the check boxes next to the appropriate check box in the **Find and List** window; then, click **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 To delete a single security profile, perform one of the following tasks:

a) In the **Find and List** window, check the check box next to the appropriate security profile; then, click **Delete Selected**.

Step 5 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Find Phones with Phone Security Profiles

To find the phones that use a specific security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 From the first drop-down list, choose the search parameter **Security Profile**.

a) From the drop-down list, choose a search pattern.

b) Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the **Rows per Page** drop-down list.

Step 4 From the list of records that display, click the link for the record that you want to view.

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

The window displays the record that you choose.