CHAPTER 5

Configuring a Phone Security Profile

This chapter contains information on the following topics:

Phone Security Profile Overview

Cisco 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 Cisco 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.

Configuration Tips for Phone Security Profiles

Consider the following information when you configure phone security profiles in Cisco Unified Communications Manager Administration:

- When you configure phones, you must select a security profile in the Phone Configuration window. If the device does not support security, apply the nonsecure profile.

- You cannot delete or change predefined, nonsecure 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 reconfigured settings apply to all phones that are assigned that profile.
- You can rename security files that are assigned to devices. The phones that are assigned the old profile name and settings assume the new profile name and settings.
- The CAPF settings in the Phone Security Profile, authentication mode and key size, also display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacture-installed certificates (MICs) or locally significant certificates (LSCs). You can update these fields directly in the Phone Configuration window.
  - If you update the CAPF settings in the security profile, the settings get updated in the Phone Configuration window.
  - If you update the CAPF settings in the Phone Configuration window and a matching profile is found, Cisco Unified Communications Manager applies the matching profile to the phone.
  - If you update the CAPF settings in the Phone Configuration window, and no matching profile is found, Cisco Unified Communications Manager creates a new profile and applies the new profile to the phone.
- If you configured the device security mode prior to a Cisco Unified Communications Manager 5.0 or later upgrade, Cisco Unified Communications Manager creates a profile that is based on the model and protocol and applies the profile to the device.
- Cisco recommends using manufacturer-installed certificates (MICs) for LSC installation only. Cisco supports LSCs to authenticate the TLS connection with Cisco Unified Communications Manager. Because MIC root certificates can be compromised, customers 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.

  Cisco recommends upgrading Cisco Unified IP Phone models 7906G, 7911G, 7931G (SCCP only), 7941G, 7941G,-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 797G, 7971G, 7971G-GE, and 7975G to use LSCs for TLS connection to Cisco Unified Communications Manager and removing MIC root certificates from the CallManager trust store to avoid possible future compatibility issues. See "Certificates" section on page 1-14 for more information.

Finding a Phone Security Profile

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

Procedure

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

The Find and List Phone Security Profile window displays. Records from an active (prior) query may also display in the window.

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

To filter or search records

- From the first drop-down list box, choose a search parameter.

- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 5-11.

Configuring a Phone Security Profile

To add, update, or copy a security profile, perform the following procedure:

Procedure

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

Step 2 Perform one of the following tasks:

- To add a new profile, click **Add New** in the Find window and continue with Step 3.
- To copy an existing security profile, locate the appropriate profile as described in "Finding a Phone Security Profile" section on page 5-2, click the **Copy** button next to the security profile that you want to copy, and continue with Step 3.
- To update an existing profile, locate the appropriate security profile as described in "Finding a Phone Security Profile" section on page 5-2 and continue with Step 3.

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

Step 3 Enter the appropriate settings as described in Table 5-1 for phones that are running SCCP or Table 5-2 for phones that are running SIP.

Step 4 Click **Save**.

Next Steps

After you create the security profile, apply it to the phone, as described in the "Applying a Phone Security Profile" section on page 5-9.

If you configured digest authentication in the phone security profile for a phone that is running SIP, you must configure the digest credentials in the End User Configuration window. You then must associate the user with the phone by using the Digest User setting in the Phone Configuration window.

Additional Information

See the "Related Topics" section on page 5-11.

Phone Security Profile Configuration Settings

Table 5-1 describes the settings for the security profile for the phone that is running SCCP.

Table 5-2 describes the settings for the security profile the phone that is running SIP.

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

- For configuration tips, see the "Configuration Tips for Phone Security Profiles" section on page 5-1.
- For related information and procedures, see the "Related Topics" section on page 5-11.

Table 5-1 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 box 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.
Device Security Mode	From the drop-down list box, choose one of the following options: • **Non Secure**—No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified Communications Manager. • **Authenticated**—Cisco Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Cisco 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.
TFTP Encrypted Config	When this check box is checked, Cisco Unified Communications Manager encrypts phone downloads from the TFTP server. Refer to "Configuration File Encryption" section on page 1-23, and "Configuring Encrypted Phone Configuration Files" procedure on page 8-1, for more information.

Table 5-1 Security Profile for Phone That is Running SCCP (continued)

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/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**— Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via 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 even though a MIC and 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 via the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via 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 (see "Configuration Tips for Phone Security Profiles" section on page 5-1, for more details). Refer to the *Cisco Unified Communications Manager Administration Guide* for information about configuring these settings on the Phone Configuration window.

Table 5-1 Security Profile for Phone That is Running SCCP (continued)

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. The other key size option 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 (see "Configuration Tips for Phone Security Profiles" section on page 5-1 for more details). Refer to the *Cisco Unified Communications Manager Administration Guide* for configuring these settings on the Phone Configuration window.

Table 5-2 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 box 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, Cisco 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.
Device Security Mode	From the drop-down list box, choose one of the following options: • **Non Secure**—No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified Communications Manager. • **Authenticated**—Cisco Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Cisco 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.

Table 5-2 Security Profile for Phone That is Running SIP (continued)

Setting	Description
Transport Type	When Device Security Mode is **Non Secure**, choose one of the following options from the drop-down list box (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 SIP phones. If Device Security Mode cannot be configured in the profile, the transport type specifies UDP.
Enable Digest Authentication	If you check this check box, Cisco Unified Communications Manager challenges all SIP requests from the phone. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of authenticated or encrypted to use these features. **Note** For more information on digest authentication, see "Digest Authentication" section on page 1-18 and "Configuring Digest Authentication for the SIP Phone" section on page 9-1.
TFTP Encrypted Config	When this check box is checked, Cisco Unified Communications Manager encrypts phone downloads from the TFTP server. This option exists for Cisco phones only. **Tip** Cisco recommends that you enable this option and configure a symmetric key to secure digest credentials and administrative passwords. Refer to "Configuration File Encryption" section on page 1-23, and "Configuring Encrypted Phone Configuration Files" section on page 8-1, for more information.
Exclude Digest Credentials in Configuration File	When this check box is checked, Cisco Unified Communications Manager omits digest credentials in phone downloads from the TFTP server. This option exists for Cisco Unified IP Phones 7905G, 7912G, 7940G, and 7960G (SIP only). Refer to "Configuration File Encryption" section on page 1-23, and "Configuring Encrypted Phone Configuration Files" section on page 8-1, for more information.

Table 5-2 Security Profile for Phone That is Running SIP (continued)

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 box, choose one of the following options: • **By Authentication String**—Installs/upgrades or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**— Installs/upgrades or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**— Installs/upgrades or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via 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 even though a MIC and 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 via the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs/upgrades or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via 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 (see "Configuration Tips for Phone Security Profiles" section on page 5-1 for more details). Refer to the *Cisco Unified Communications Manager Administration Guide* for information about configuring these settings in the Phone Configuration window.

Table 5-2 Security Profile for Phone That is Running SIP (continued)

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. The other key size option 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 (see "Configuration Tips for Phone Security Profiles" section on page 5-1 for more details). Refer to the *Cisco Unified Communications Manager Administration Guide* for information about configuring these settings in the Phone Configuration window.
SIP Phone Port	This setting applies to phones that are running SIP that use UDP transport. Enter the port number for Cisco Unified IP Phones (SIP only) that use UDP to listen for SIP messages from Cisco Unified Communications Manager. The default setting equals 5060. Phones that use TCP or TLS ignore this setting.

Applying a Phone Security Profile

You apply a phone security profile to the phone in the Phone Configuration window.

Before You Begin

Before you apply a security profile that uses certificates for authentication of the phone, ensure that phone contains a locally significant certificate (LSC) or manufacture-installed certificate (MIC).

If the phone does not contain a certificate, perform the following steps:

1. In the Phone Configuration window, apply a nonsecure profile.
2. In the Phone Configuration window, install a certificate by configuring the CAPF settings. For more information on performing this task, see the "Using the Certificate Authority Proxy Function" section on page 7-1.
3. 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 Find the phone, as described in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 After the Phone Configuration window displays, locate the **Device Security Profile**.

Step 3 From the **Device Security Profile** drop-down list box, choose the security profile that applies to the device. Only the phone security profiles that are configured for the phone type and protocol display.

Step 4 Click **Save**.

Step 5 To reset the phone, click **Reset**.

Next Steps

If you configured digest authentication for phones that are running SIP, you must configure the digest credentials in the End User Configuration window. Then, you must configure the Digest User setting in the Phone Configuration window. For more information about configuring digest users and digest credentials, refer to the "Configuring Digest Authentication for the SIP Phone" section on page 9-1.

Additional Information

See the "Related Topics" section on page 5-11.

Deleting a Phone Security Profile

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

Before You Begin

Before you can delete a security profile from Cisco Unified Communications Manager Administration, 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, choose **Dependency Records** from the Related Links drop-down list box in the Security Profile Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, go to **System > Enterprise Parameters** 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, refer to the *Cisco Unified Communications Manager System Guide.*

Procedure

Step 1 Find the security profile by using the procedure in the "Finding a Phone Security Profile" section on page 5-2.

Step 2 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 3 To delete a single security profile, perform one of the following tasks:

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

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Additional Information

See the "Related Topics" section on page 5-11.

Finding Phones That Use Phone Security Profiles

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

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

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

- From the drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

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

Step 3 Click **Find**.

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

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

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

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 5-11.

Where to Find More Information

Related Topics

- Digest Authentication, page 1-18
- Configuration File Encryption, page 1-23
- Phone Security Profile Overview, page 5-1
- Configuration Tips for Phone Security Profiles, page 5-1
- Finding a Phone Security Profile, page 5-2
- Configuring a Phone Security Profile, page 5-3
- Phone Security Profile Configuration Settings, page 5-4

- Applying a Phone Security Profile, page 5-9
- Deleting a Phone Security Profile, page 5-10
- Finding Phones That Use Phone Security Profiles, page 5-11
- Configuring Encrypted Phone Configuration Files, page 8-1
- Configuring Digest Authentication for the SIP Phone, page 9-1
- Phone Hardening, page 10-1

Related Cisco Documentation

Cisco Unified Communications Manager Administration Guide

Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager