



Configuring a Phone Security Profile

This chapter contains information on the following topics:

- [Phone Security Profile Overview, page 5-1](#)
- [Finding a SCCP or SIP Phone Security Profile, page 5-2](#)
- [Configuring the SCCP or SIP Phone Security Profile, page 5-2](#)
- [SCCP Phone Security Profile Configuration Settings, page 5-3](#)
- [SIP Phone Security Profile Configuration Settings, page 5-5](#)
- [Applying a SCCP or SIP Phone Security Profile, page 5-8](#)
- [Deleting a SCCP or SIP Phone Security Profile, page 5-9](#)
- [Finding Phones that Use Phone Security Profiles, page 5-10](#)
- [Where to Find More Information, page 5-10](#)

Phone Security Profile Overview

Cisco Unified CallManager Administration groups security-related settings, for example, device security mode, digest authentication, and some CAPF settings, so you can apply all configured settings to a SIP or SCCP phone when you choose the profile in the device configuration window.

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

- Configure the CAPF settings in the profile in conjunction with the Certificate Authority Proxy Function settings that display in the Phone Configuration window.
- All SIP and SCCP phones require that you apply a security profile. If the device does not support security, apply a nonsecure profile.
- If you configured the device security mode prior to the Cisco Unified CallManager 5.0 upgrade, Cisco Unified CallManager creates a profile based on the mode and applies the profile to the device.
- If the device does not support the profile that you configure, Cisco Unified CallManager does not allow you to apply it to the device.

Finding a SCCP or SIP Phone Security Profile

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Security Profile > SIP Phone Security Profile** or **SCCP Phone Security Profile**.

The Find and List window displays.

Step 2 From the drop-down list boxes, choose your search criteria for the security profiles that you want to list and click **Find**.



Note To find all security profiles that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the security profiles that match your search criteria.

Step 3 Click the **Name** link for the security profile that you want to view.



Tip To search for the Name or Description within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the “[Related Topics](#)” section on page 5-10.

Configuring the SCCP or SIP Phone Security Profile

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Security Profile > SIP Phone Security Profile** or **SCCP Phone Security Profile**.

Step 2 Perform one of the following tasks:

- To add a new profile, click the **Add New** button and continue with [Step 3](#).
- To copy an existing security profile, locate the appropriate profile as described in “[Finding a SCCP or SIP 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 SCCP or SIP Phone Security Profile](#)” section on page 5-2 and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 5-1](#) for SCCP phones or [Table 5-2](#) for SIP phones.

Step 4 Click **Save**.

Additional Steps

After you create the security profile, apply it to the phone, as described in the [“Applying a SCCP or SIP Phone Security Profile”](#) section on page 5-8.

If you configured digest authentication in the phone security profile for the SIP phone, you must configure the digest credentials in the End User Configuration window. You specify the digest user in the Phone Configuration window. For more information about configuring digest users and digest credentials, refer to [“Configuring Digest Authentication for the SIP Phone”](#) section on page 8-1.

Additional Information

See the [“Related Topics”](#) section on page 5-10.

SCCP Phone Security Profile Configuration Settings

Table 5-1 describes the settings for the SCCP Phone Security Profile.

Table 5-1 SCCP Phone Security Profile

Setting	Description
Name	Enter a name for the security profile. If the device supports the profile, the name displays in the SCCP Phone Security Profile drop-down list box in the Phone Configuration window.
Description	Enter a description for the security profile.
Device Security Mode	From the drop-down list box, choose one of the following options: <ul style="list-style-type: none"> • Non Secure—No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified CallManager. • Authenticated—Cisco Unified CallManager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens. • Encrypted—Cisco Unified CallManager 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.

Table 5-1 SCCP Phone Security Profile (continued)

Setting	Description
Authentication Mode	<p>Used for the Certificate Authority Proxy Function, this field allows you to choose the method by which you want the phone to authenticate with CAPF during the certificate operation, which you configure in the Phone Configuration window.</p> <p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • 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. <p>This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Key Size	<p>Used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048.</p> <p>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.</p>

SIP Phone Security Profile Configuration Settings

Table 5-2 describes the settings for the SIP Phone Security Profile.

Table 5-2 SIP Phone Security Profile

Setting	Description
Name	<p>Enter a name for the security profile.</p> <p>Tip To ensure that you apply the correct profile to the device, include the device model in the security profile name.</p>
Description	Enter a description for the security profile.
Nonce Validity Time	<p>A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.</p> <p>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 CallManager generates a new value.</p>
Device Security Mode	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • Non Secure—No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified CallManager. • Authenticated—Cisco Unified CallManager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens. • Encrypted—Cisco Unified CallManager 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.
Transport Type	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • TCP—Choose the Transmission Control Protocol to ensure that packets get received in the same order 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 that they are sent. This protocol does not provide any security. • TLS—Choose the Transport Layer Security protocol to ensure signaling integrity, device authentication, and signaling encryption for SIP phones. <ul style="list-style-type: none"> For devices that support authentication only, the TLS_RSA_WITH_NULL_SHA algorithm gets used. For devices that support authentication and encryption, the TLS_RSA_WITH_AES128_SHA gets used. • TCP + UDP—Choose this option if you want to use a combination of TCP and UDP. This option does not provide any security.

Table 5-2 SIP Phone Security Profile (continued)

Setting	Description
Enable Digest Authentication	<p>If you want Cisco Unified CallManager to challenge the identity of the phone when it sends a request to Cisco Unified CallManager, check this check box. After Cisco Unified CallManager challenges the identity, the phone responds with a MD5 checksum, and Cisco Unified CallManager verifies the information based on the credentials that you configured in Cisco Unified CallManager Administration. If the credentials match, digest authentication of the phone is successful.</p> <p>If you check this check box, Cisco Unified CallManager challenges all SIP requests from the phone.</p> <p>Tip You specify digest authentication credentials in the End User window in Cisco Unified CallManager Administration. To associate the credentials with the phone after you configure the user, you choose a Digest User, an end user, in the Phone Configuration window.</p> <p>Digest authentication does not provide integrity or confidentiality. To ensure integrity and confidentiality for the phone, configure the Transport Type as TLS and the device security mode as encrypted.</p> <p>Note For more information on digest authentication, see the “Digest Authentication” section on page 1-16 and Chapter 8, “Configuring Digest Authentication for the SIP Phone”.</p>

Table 5-2 SIP Phone Security Profile (continued)

Setting	Description
Authentication Mode	<p>Used for CAPF, this field allows you to choose the method by which you want the phone to authenticate with CAPF during the certificate operation, which you configure in the Phone Configuration window.</p> <p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • 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. <p>This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.</p> • 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. <p>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.</p> <p>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.</p> • 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. <p>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.</p>

Table 5-2 SIP Phone Security Profile (continued)

Setting	Description
Key Size	Used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. 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.
SIP Phone Port	Enter the port number that you want Cisco Unified SIP IP Phones to use to listen for SIP messages from Cisco Unified CallManager. The default setting equals 5060.

Applying a SCCP or SIP Phone Security Profile

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

Before you apply a security profile that is configured for authentication or encryption, 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 6-1](#).
3. In the Phone Configuration window, apply a 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 CallManager Administration Guide*.
 - Step 2** After the Phone Configuration window displays, locate the following settings, depending on your phone protocol:
 - **SCCP Phone Security Profile**
 - **SIP Phone Security Profile**
 - Step 3** From the security profile drop-down list box, choose the security profile that applies to the device.
 - Step 4** Click **Save**.
 - Step 5** To reset the phone, click **Reset**.
-

Additional Steps

If you configured digest authentication for SIP phones, 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 [“Configuring Digest Authentication for the SIP Phone” section on page 8-1](#).

Additional Information

See the [“Related Topics” section on page 5-10](#).

Deleting a SCCP or SIP Phone Security Profile

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

Before You Begin

Before you can delete a security profile from Cisco Unified CallManager 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, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that relates to the dependency records feature. For more information about dependency records, refer to the *Cisco Unified CallManager System Guide*.

Procedure

-
- Step 1** Find the security profile by using the procedure in the [“Finding a SCCP or SIP 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 the **Delete Selected** icon or the **Delete Selected** button.
- 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 the **Delete Selected** icon or the **Delete Selected** button.
 - In the Find and List window, click the Name link for the security profile. After the specific Security Profile Configuration window displays, click the **Delete** icon or the **Delete** button.
- 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 5-10](#).

Finding Phones that Use Phone Security Profiles

To find a phone that uses the Phone Security Profile, perform the following procedure:

-
- Step 1** In Cisco Unified CallManager Administration, choose **Device > Phone**.
 - Step 2** From the Find Phone where drop-down list box, choose **Security Profile**.
 - Step 3** If you want to do so, specify additional search criteria for the security profile by choosing an option in the drop-down list box next to the Find Phone drop-down list box; then, enter the specific search criteria.
 - Step 4** After you specify your search criteria, click **Find**. The search results display.
-

Additional Information

See the [“Related Topics”](#) section on page 5-10.

Where to Find More Information

Related Topics

- [Phone Security Profile Overview, page 5-1](#)
- [Finding a SCCP or SIP Phone Security Profile, page 5-2](#)
- [Configuring the SCCP or SIP Phone Security Profile, page 5-2](#)
- [SCCP Phone Security Profile Configuration Settings, page 5-3](#)
- [SIP Phone Security Profile Configuration Settings, page 5-5](#)
- [Applying a SCCP or SIP Phone Security Profile, page 5-8](#)
- [Deleting a SCCP or SIP Phone Security Profile, page 5-9](#)
- [Finding Phones that Use Phone Security Profiles, page 5-10](#)
- [Phone Hardening, page 9-1](#)

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager