



Configuring the SIP Trunk Security Profile

This chapter contains information on the following topics:

- [SIP Trunk Security Profile Overview, page 14-1](#)
- [Finding a SIP Trunk Security Profile, page 14-1](#)
- [Configuring the SIP Trunk Security Profile, page 14-2](#)
- [SIP Trunk Security Profile Configuration Settings, page 14-3](#)
- [Applying a SIP Trunk Security Profile, page 14-6](#)
- [Deleting a SIP Trunk Security Profile, page 14-6](#)
- [Where to Find More Information, page 14-7](#)

SIP Trunk Security Profile Overview

Cisco Unified CallManager Administration groups SIP trunk security-related settings, for example, device security mode, digest authentication, and incoming/outgoing transport type settings, so you can apply all configured settings to a SIP trunk when you choose the profile in the SIP Trunk Configuration window. All SIP trunks require that you apply a security profile. If the SIP trunk does not support security, apply a nonsecure profile.

Finding a SIP Trunk Security Profile

To find a SIP trunk security profile, perform the following procedure:

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, choose **System > Security Profile > SIP Trunk 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 SIP trunk 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 14-7](#).

Configuring the SIP Trunk Security Profile

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

Procedure

- Step 1** In Cisco Unified CallManager Administration, choose **System > Security Profile > SIP Trunk 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 SIP Trunk Security Profile” section on page 14-1](#), 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 SIP Trunk Security Profile” section on page 14-1](#) and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 14-1](#).
- Step 4** Click **Save**.

Additional Steps

After you create the security profile, apply it to the trunk, as described in the [“Applying a SIP Trunk Security Profile” section on page 14-6](#).

If you configured digest authentication for SIP trunks, you must configure the digest credentials in the SIP Realm window for the trunk and Application User window for applications that are connected through the SIP trunk, if you have not already done so.

If you enabled application-level authorization SIP trunks, you must configure the methods allowed for the trunk in the Application User window.

Additional Information

See the “[Related Topics](#)” section on page 14-7.

SIP Trunk Security Profile Configuration Settings

Table 14-1 describes the settings for the SIP Trunk Security Profile. Refer to the “[Interactions](#)” section on page 1-6 for descriptions of method authorizations in Cisco Unified CallManager.

Table 14-1 SIP Trunk Security Profile Configuration Settings

Setting	Description
Name	Enter a name for the security profile. The name displays in the SIP Trunk Security Profile drop-down list box in the Trunk Configuration window.
Description	Enter a description for the security profile.
Incoming Transport Type	From the drop-down list box, choose the incoming transport mode. Tip The Transport Layer Security (TLS) protocol secures the connection between Cisco Unified CallManager and the trunk. If you choose the TLS option, make sure that you choose the TLS option from the Outgoing Transport Type drop-down list box.
Outgoing Transport Type	From the drop-down list box, choose the outgoing transport mode. If you chose TLS for the Incoming Transport Type, you must choose TLS for the Outgoing Transport Type. Tip Choose the Transport Layer Security protocol to ensure signaling integrity, device authentication, and signaling encryption for SIP trunks.
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 apply. A TCP or UDP connection opens to Cisco Unified CallManager. • Authenticated—Cisco Unified CallManager provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • Encrypted—Cisco Unified CallManager provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling. Tip SIP trunks support signaling encryption (not SRTP).

Table 14-1 SIP Trunk Security Profile Configuration Settings (continued)

Setting	Description
Enable Digest Authentication	<p>If you want Cisco Unified CallManager to challenge the identity of the SIP user agent that connects to the trunk, check this check box. After Cisco Unified CallManager challenges the identity, the trunk responds with a MD5 checksum, username, password, nonce value, and requested URI, 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 succeeded.</p> <p>If you check this check box, Cisco Unified CallManager challenges all SIP requests from the trunk.</p> <p>Digest authentication does not provide integrity or confidentiality. To ensure integrity and confidentiality for the trunk, configure the TLS protocol.</p>
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>
X.509 Subject Name	<p>This field applies if you configured TLS for the incoming and outgoing transport type.</p> <p>For the authenticated device that connects to the SIP trunk, enter the subject name of the X.509 certificate. If you have a Cisco Unified CallManager cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts, which results in multiple X.509 subject names for the trunk. If multiple X.509 subject names exist, enter one of the following characters to separate the names: space, comma, semicolon, or a colon.</p> <p>You can enter up to 4096 characters in this field.</p> <p>Tip The subject name corresponds to the source connection TLS certificate. Ensure subject names are unique for each subject name and port. You cannot assign the same subject name and incoming port combination to different SIP trunks.</p> <p>Example: SIP TLS trunk1 on port 5061 has X.509 Subject Names my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has X.509 Subject Names my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have X.509 Subject Name my_ccm4 but cannot have X.509 Subject Name my_cm1.</p>
Incoming Port	<p>Choose the incoming port. Enter a value that is a unique port number from 1024-65535. The default port value for incoming TCP and UDP SIP messages specifies 5060.</p> <p>The value that you enter applies to all SIP trunks that use the profile. If you want to do so, you can configure the same incoming port number for all SIP trunks.</p>

Table 14-1 SIP Trunk Security Profile Configuration Settings (continued)

Setting	Description
Enable Application Level Authorization	<p>If you check this check box, you must check the Enable Digest Authentication check box and configure digest authentication for the trunk. For information on configuring digest authentication for the trunk, see the “Configuring Digest Authentication for the SIP Trunk” section on page 15-1.</p> <p>If you check this check box, trunk-level authorization occurs first and then application-level authorization occurs. Application-level authorization occurs for SIP messages that come from applications on the SIP user agent. Application-level authorization is based on the authorization check boxes that you check in the Application User Configuration window (User Management > Application User).</p> <p>Tip Consider using application-level authorization if you do not trust the identity of the application or if the application is not trusted on a particular trunk; that is, application requests may come from a different trunk than you expect.</p>
Accept Presence Subscription	<p>If you want Cisco Unified CallManager to accept presence subscription requests that come via the SIP trunk, check this check box.</p> <p>If you checked the Enable Application Level Authorization check box, go to the Application User Configuration window and check the Accept Presence Subscription check box for any application users that are authorized for this feature.</p> <p>When application-level authorization is enabled, if you check the Accept Presence Subscription check box for the application user but not for the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.</p>
Accept Out-of-Dialog Refer	<p>If you want Cisco Unified CallManager to accept incoming non-INVITE, Out-of-Dialog REFER requests that come via the SIP trunk, check this check box.</p> <p>If you checked the Enable Application Level Authorization check box, go to the Application User Configuration window and check the Accept Out-of-Dialog Refer check box for any application users that are authorized for this method.</p>
Accept Unsolicited Notification	<p>If you want Cisco Unified CallManager to accept incoming non-INVITE, unsolicited notification messages that come via the SIP trunk, check this check box.</p> <p>If you checked the Enable Application Level Authorization check box, go to the Application User Configuration window and check the Accept Unsolicited Notification check box for any application users that are authorized for this method.</p>
Accept Header Replacement	<p>If you want Cisco Unified CallManager to accept new SIP dialogs, which have replaced existing SIP dialogs, check this check box.</p> <p>If you checked the Enable Application Level Authorization check box, go to the Application User Configuration window and check the Accept Header Replacement check box for any application users that are authorized for this method.</p>

Applying a SIP Trunk Security Profile

You apply a SIP trunk security profile to the trunk in the Trunk Configuration window. To apply a security profile to a device, perform the following procedure:

Procedure

- Step 1** Find the trunk, as described in the *Cisco Unified CallManager Administration Guide*.
 - Step 2** After the Trunk Configuration window displays, locate the **SIP Trunk Security Profile** setting.
 - 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 trunks, you must configure the digest credentials in the SIP Realm window for the trunk and Application User window for applications that are connected through the SIP trunk, if you have not already done so. See “[Configuring a SIP Realm](#)” section on [page 15-4](#).

Additional Information

See the “[Related Topics](#)” section on [page 14-7](#).

Deleting a SIP Trunk Security Profile

This section describes how to delete a SIP trunk 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 SIP Trunk 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 is related 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 SIP Trunk Security Profile](#)” section on [page 14-1](#).
- 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 Selected** icon or the **Delete Selected** 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 14-7.

Where to Find More Information

Related Topics

- [SIP Trunk Security Profile Overview, page 14-1](#)
- [Finding a SIP Trunk Security Profile, page 14-1](#)
- [Configuring the SIP Trunk Security Profile, page 14-2](#)
- [SIP Trunk Security Profile Configuration Settings, page 14-3](#)
- [Applying a SIP Trunk Security Profile, page 14-6](#)
- [Deleting a SIP Trunk Security Profile, page 14-6](#)

Related Cisco Documentation

Cisco Unified CallManager Administration Guide

