Configuring the SIP Trunk Security Profile

This chapter contains information on the following topics:

SIP Trunk Security Profile Overview

Cisco Unified CallManager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings. You apply the configured settings to the SIP trunk when you choose the security profile in the Trunk Configuration window.

Installing Cisco Unified CallManager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile.

Only security features that the SIP trunk supports display in the security profile settings window.

Configuration Tips for SIP Trunk Security Profile

Consider the following information when you configure SIP trunk security profiles in Cisco Unified CallManager Administration:

- When you are configuring a SIP trunk, you must select a security profile in the Trunk Configuration window. If the device does not support security, apply a nonsecure profile.
- 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 SIP trunk, the reconfigured settings apply to all SIP trunks that are assigned that profile.
- You can rename security files that are assigned to devices. The SIP trunks that are assigned the old profile name and settings assume the new profile name and settings.
- If you configured the device security mode prior to a Cisco Unified CallManager 5.0 or later upgrade, Cisco Unified CallManager creates a profile for the SIP trunk and applies the profile to the device.

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 14-8.

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 14-2, 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 SIP Trunk Security Profile" section on page 14-2 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 14-7.

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 for applications that are connected through the SIP trunk, you must configure the methods that are allowed for the application in the Application User window, if you have not already done so.

Additional Information

See the "Related Topics" section on page 14-8.

SIP Trunk Security Profile Configuration Settings

Table 14-1 describes the settings for the SIP Trunk Security Profile.

- For configuration tips, refer to the "Configuration Tips for SIP Trunk Security Profile" section on page 14-1.
- For related information and procedures, see the "Related Topics" section on page 14-8.

Table 14-1 SIP Trunk Security Profile Configuration Settings

Setting	Description
Name	Enter a name for the security profile. When you save the new 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.

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

Setting	Description
Device Security Mode	From the drop-down list box, choose one of the following options: • **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. **Note** SIP trunks support signaling encryption (not SRTP).
Incoming Transport Type	When Device Security Mode is **Non Secure**, TCP+UDP specifies the transport type. When Device Security Mode is **Authenticated** or **Encrypted**, TLS specifies the transport type. **Note** The Transport Layer Security (TLS) protocol secures the connection between Cisco Unified CallManager and the trunk.
Outgoing Transport Type	From the drop-down list box, choose the outgoing transport mode. When Device Security Mode is **Non Secure,** choose TCP or UDP. When Device Security Mode is **Authenticated** or **Encrypted**, TLS specifies the transport type. **Note** TLS ensures signaling integrity, device authentication, and signaling encryption for SIP trunks.
Enable Digest Authentication	Check this check box to enable digest authentication. If you check this check box, Cisco Unified CallManager challenges all SIP requests from the trunk. Digest authentication does not provide device authentication, integrity or confidentiality.Choose a security mode of authenticated or encrypted to use these features. For more information on digest authentication, see the Digest Authentication, page 1-16, and Configuring Digest Authentication for the SIP Trunk, page 15-1. **Tip** Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.
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 CallManager 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.

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

Setting	Description
X.509 Subject Name	This field applies if you configured TLS for the incoming and outgoing transport type. For device authentication, enter the subject name of the X.509 certificate for the SIP trunk device. 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. You can enter up to 4096 characters in this field. **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. 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.
Incoming Port	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. The default SIP secured port for incoming TLS messages specifies 5061. The value that you enter applies to all SIP trunks that use the profile. **Tip** All SIP trunks that use TLS can share the same incoming port; all SIP trunks that use TCP + UDP can share the same incoming port. You cannot mix SIP TLS transport trunks with SIP non-TLS transport trunk types on the same port.

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

Setting	Description
Enable Application Level Authorization	Application-level authorization applies to applications that are connected through the SIP trunk. If you check this check box, you must also check the Enable Digest Authentication check box and configure digest authentication for the trunk. Cisco Unified CallManager authenticates a SIP application user before checking the allowed application methods. When application level authorization is enabled, trunk-level authorization occurs first, and application-level authorization then occurs, meaning Cisco Unified CallManager checks the methods that are authorized for the trunk (in this security profile) before the methods that are authorized for the SIP application user in the Application User Configuration window. **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. For information on configuring digest authentication for the trunk, see the Configuring Digest Authentication for the SIP Trunk, page 15-1. For more information about authorization, refer to Authorization, page 1-17, and Interactions, page 1-6. For more information about configuring application level authorization at the Application User Configuration window, see the *Cisco Unified CallManager Administration Guide*.
Accept Presence Subscription	If you want Cisco Unified CallManager to accept presence subscription requests that come via the SIP trunk, check this check box. 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. 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.
Accept Out-of-Dialog Refer	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. 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.

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

Setting	Description
Accept Unsolicited Notification	If you want Cisco Unified CallManager to accept incoming non-INVITE, unsolicited notification messages that come via the SIP trunk, check this check box. 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.
Accept Header Replacement	If you want Cisco Unified CallManager to accept new SIP dialogs, which have replaced existing SIP dialogs, check this check box. 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.

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 trunk, click **Reset**.

Additional Steps

If you applied a profile enabling digest authentication for SIP trunks, you must configure the digest credentials in the SIP Realm window for the trunk. See "Configuring a SIP Realm" section on page 15-4.

If you applied a profile enabling application-level authorization, you must configure the digest credentials and allowed authorization methods in the Application User window, if you have not already done so.

Additional Information

See the "Related Topics" section on page 14-8.

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 14-2.

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 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 14-8.

Where to Find More Information

Related Topics

- SIP Trunk Security Profile Overview, page 14-1
- Configuration Tips for SIP Trunk Security Profile, page 14-1
- Finding a SIP Trunk Security Profile, page 14-2
- 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 14-7

- Deleting a SIP Trunk Security Profile, page 14-8
- Authorization, page 1-17
- Interactions, page 1-6
- Digest Authentication, page 1-16

Related Cisco Documentation

Cisco Unified CallManager Administration Guide

Cisco Unified CallManager System Guide