



SIP Trunk Security Profile Setup

This chapter provides information about SIP trunk security profile setup.

- [About SIP Trunk Security Profile Setup, on page 1](#)
- [SIP Trunk Security Profile Setup Tips, on page 1](#)
- [Find SIP Trunk Security Profile, on page 2](#)
- [Set Up SIP Trunk Security Profile, on page 2](#)
- [SIP Trunk Security Profile Settings, on page 3](#)
- [Apply SIP Trunk Security Profile, on page 8](#)
- [Synchronize SIP Trunk Security Profile with SIP Trunks, on page 9](#)
- [Delete SIP Trunk Security Profile, on page 9](#)
- [Where to Find More Information About SIP Trunk Security Profiles, on page 10](#)

About SIP Trunk Security Profile Setup

Unified Communications Manager 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 Unified Communications Manager 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.

SIP Trunk Security Profile Setup Tips

Consider the following information when you configure SIP trunk security profiles in Unified Communications Manager 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 Unified Communications Manager 5.0 or later upgrade, Unified Communications Manager creates a profile for the SIP trunk and applies the profile to the device.

Find SIP Trunk Security Profile

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

Procedure

Step 1 Choose **System** > **Security Profile** > **SIP Trunk Security Profile**.

The **Find and List** 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, on page 2](#).

To filter or search records

- a) From the drop-down list box, choose a search parameter.
- b) Then from the drop-down list box, 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 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.

Set Up SIP Trunk Security Profile

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

Procedure

- Step 1** From Cisco Unified Communications Manager Administration, choose **System > Security Profile > SIP Trunk Security Profile**.
- Step 2** Perform one of the following tasks:
- To add a new profile, click **Add New** in the **Find** window.
(You can also display a profile and then click **Add New**.)
The configuration window displays the default settings for each field.
 - To copy an existing security profile, locate the appropriate profile and click the **Copy** icon for that record in the Copy column.
(You can also display a profile and then click **Copy**.)
The configuration window displays the configured settings.
 - To update an existing profile, locate and display the appropriate security profile as described in [Find SIP Trunk Security Profile, on page 2](#).
The configuration window displays the current settings.
- Step 3** Enter the appropriate settings as described in SIP Trunk Security Profile Settings.
- Step 4** Click **Save**.
After you create the security profile, apply it to the trunk. 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.

SIP Trunk Security Profile Settings

The following table describes the settings for the SIP Trunk Security Profile.

Table 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 in the Trunk Configuration window.
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	<p>From the drop-down list, choose one of the following options:</p> <ul style="list-style-type: none"> • Non Secure—No security features except image authentication apply. A TCP or UDP connection opens to Unified Communications Manager. • Authenticated—Unified Communications Manager provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • Encrypted— Unified Communications Manager provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling. <p>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).</p> <p>These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher.</p> <p>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.</p>
Incoming Transport Type	<p>When Device Security Mode is Non Secure TCP+UDP specifies the transport type.</p> <p>When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type.</p> <p>Note The Transport Layer Security (TLS) protocol secures the connection between Unified Communications Manager and the trunk.</p>
Outgoing Transport Type	<p>From the drop-down list, choose the outgoing transport mode.</p> <p>When Device Security Mode is Non Secure, choose TCP or UDP.</p> <p>When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type.</p> <p>Note TLS ensures signaling integrity, device authentication, and signaling encryption for SIP trunks.</p> <p>Tip You must use UDP as the outgoing transport type when connecting SIP trunks between Unified Communications Manager systems and IOS gateways that do not support TCP connection reuse.</p>

Setting	Description
Enable Digest Authentication	<p>Check this check box to enable digest authentication. If you check this check box, Unified Communications Manager challenges all SIP requests from the trunk.</p> <p>Digest authentication does not provide device authentication, integrity or confidentiality. Choose a security mode of Authenticated or Encrypted to use these features.</p> <p>Tip Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.</p>
Nonce Validity Time	<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, Unified Communications Manager generates a new value.</p> <p>Note A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.</p>
Secure Certificate Subject or Subject Alternate Name	<p>This field applies if you configured TLS for the incoming and outgoing transport type.</p> <p>For device authentication, enter the name of the Secure Certificate Subject or Subject Alternate Name certificate for the SIP trunk device. If you have a Unified Communications Manager cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts, which results in multiple Secure Certificate Subject or Subject Alternate Name for the trunks. If multiple Secure Certificate Subject or Subject Alternate Name exists, 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. Example: SIP TLS trunk1 on port 5061 has Secure Certificate Subject or Subject Alternate Name my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has Secure Certificate Subject or Subject Alternate Name my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have Secure Certificate Subject or Subject Alternate Name my_ccm4 but cannot have Secure Certificate Subject or Subject Alternate Name my_cm1.</p>

Setting	Description
Incoming Port	<p>Choose the incoming port. Enter a value that is a unique port number from 0-65535. 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.</p> <p>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.</p> <p>Tip If the incoming packet rate on a SIP trunk UDP port from a single IP address exceeds the configured SIP Trunk UDP Port Throttle Threshold during normal traffic, reconfigure the threshold. When a SIP trunk and SIP station share the same incoming UDP port, Unified Communications Manager throttles packets based on the higher of the two service parameter values. You must restart the Cisco CallManager service for changes to this parameter to take effect.</p>
Enable Application Level Authorization	<p>Application-level authorization applies to applications that are connected through the SIP trunk.</p> <p>If you check this check box, you must also check the Enable Digest Authentication check box and configure digest authentication for the trunk. Unified Communications Manager authenticates a SIP application user before checking the allowed application methods.</p> <p>When application level authorization is enabled, trunk-level authorization occurs first, and application-level authorization then occurs, which means that Unified Communications Manager 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.</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 Unified Communications Manager 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>

Setting	Description
Accept Out-of-Dialog Refer	<p>If you want Unified Communications Manager 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 Unified Communications Manager 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 Replaces Header	<p>If you want Unified Communications Manager 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>
Transmit Security Status	<p>If you want Unified Communications Manager to transmit the security icon status of a call from the associated SIP trunk to the SIP peer, check this check box.</p> <p>Default: This box is not checked.</p>
SIP V.150 Outbound SDP Offer Filtering	<p>From the drop-down list, select one of the following filter options:</p> <ul style="list-style-type: none"> • Use Default Filter—The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System > Service Parameters > Clusterwide Parameters (Device-SIP) in Cisco Unified Communications Manager Administration. • No Filtering—The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • Remove MER V.150—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified Communications Manager. • Remove Pre-MER V.150—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER-compliant devices that are incapable of processing offers with pre-MER lines.

Setting	Description
SIP V.150 Outbound SDP Offer Filtering	<p>From the drop-down list, select one of the following filter options:</p> <ul style="list-style-type: none"> • Use Default Filter—The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System > Service Parameters > Clusterwide Parameters (Device-SIP) in Cisco Unified Communications Manager Administration. • No Filtering—The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • Remove MER V.150—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified Communications Manager. • Remove Pre-MER V.150—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER compliant devices that are incapable of processing offers with pre-MER lines. <p>Note You have to configure IOS on SIP for V.150 to make a secure call connection. For more information to configure IOS on Unified Communications Manager, see http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html.</p>

Apply 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 [Administration Guide for Cisco Unified Communications Manager](#).
- Step 2** After the **Trunk Configuration** window displays, locate the **SIP Trunk Security Profile** setting.
- Step 3** From the **security profile** drop-down list, choose the security profile that applies to the device.
- Step 4** Click **Save**.
- Step 5** To reset the trunk, click **Apply Config**.
- 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. 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.
-

Synchronize SIP Trunk Security Profile with SIP Trunks

To synchronize SIP trunks with a SIP Trunk Security Profile that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, you may not need to perform a reset/restart on some affected devices.)

Procedure

- Step 1** Choose **System > Security Profile > SIP Trunk Security Profile**.
 - Step 2** Choose the search criteria to use.
 - Step 3** Click **Find**.
The window displays a list of SIP trunk security profiles that match the search criteria.
 - Step 4** Click the SIP trunk security profile to which you want to synchronize applicable SIP trunks.
 - Step 5** Make any additional configuration changes.
 - Step 6** Click **Save**.
 - Step 7** Click **Apply Config**.
The **Apply Configuration Information** dialog appears.
 - Step 8** Click **OK**.
-

Delete SIP Trunk Security Profile

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

Before you begin

Before you can delete a security profile from 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 **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 *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

- Step 1** Find the SIP trunk security profile to delete.
- Step 2** Perform one of the following tasks:

- a) To delete multiple security profiles, perform one of these tasks in the **Find and List** window:
 - Check the check boxes next to the security profiles that you want to delete; then, click **Delete Selected**.
 - You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.
- b) To delete a single security profile, perform one of these tasks in the **Find and List** window:
 - Check the check box next to the security profile that you want to delete; then, click **Delete Selected**.
 - Click the **Name** link for the security profile. After the specific Security Profile Configuration window displays, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Where to Find More Information About SIP Trunk Security Profiles

- [Authorization](#)
- [Interactions](#)
- [Digest Authentication](#)