Trunk and Gateway SIP Security

Trunk and Gateway SIP Security Overview

This section provides an overview of SIP trunk encryption, gateway encryptions and security profile setup tips.

SIP Trunk Encryption

SIP trunks can support secure calls both for signaling as well as media; TLS provides signaling encryption and SRTP provides media encryption.

To configure signaling encryption for the trunk, choose the following options when you configure the SIP trunk security profile (in the **System** > **Security Profile** > **SIP Trunk Security Profile** window):

- From the **Device Security Mode** drop-down list, choose “Encrypted.”
- From the **Incoming Transport Type** drop-down list, choose “TLS.”
- From the **Outgoing Transport Type** drop-down list, choose “TLS.”

After you configure the SIP trunk security profile, apply it to the trunk (in the **Device** > **Trunk** > **SIP Trunk** configuration window).

To configure media encryption for the trunk, check the **SRTP Allowed** check box (also in the **DeviceTrunkSIP Trunk** configuration window).

Caution If you check this check box, we recommend that you use an encrypted TLS profile, so that keys and other security-related information do not get exposed during call negotiations. If you use a non- secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Cisco IOS MGCP Gateway Encryption

Unified Communications Manager supports gateways that use the MGCP SRTP package, which the gateway uses to encrypt and decrypt packets over a secure RTP connection. The information that gets exchanged during call setup determines whether the gateway uses SRTP for a call. If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback (and vice versa) may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

When the system sets up an encrypted SRTP call between two devices, Unified Communications Manager generates a master encryption key and salt for secure calls and sends them to the gateway for the SRTP stream only. Unified Communications Manager does not send the key and salt for SRTCP streams, which the gateway also supports. These keys get sent to the gateway over the MGCP signaling path, which you should secure by using IPSec. Although Unified Communications Manager does not recognize whether an IPSec connection exists, the system sends the session keys to the gateway in the cleartext if IPSec is not configured. Confirm that the IPSec connection exists, so the session keys get sent through a secure connection.

Tip If the MGCP gateway, which is configured for SRTP, is involved in a call with an authenticated device, for example, an authenticated phone that is running SCCP, a shield icon displays on the phone because Unified Communications Manager classifies the call as authenticated. Unified Communications Manager classifies a call as encrypted if the SRTP capabilities for the devices are successfully negotiated for the call. If the MGCP gateway is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

The following are the facts about MGCP E1 PRI gateways:

- You must configure the MGCP gateway for SRTP encryption. Configure the gateway using the following command: **mgcppackage-capabilitysrtp-package**
- The MGCP gateway must specify an Advanced IP Services or Advanced Enterprise Services image.

  For example, **c3745-adventerprisek9-mz.124-6.T.bin**
- Protected status gets exchanged with the MGCP E1 PRI gateway by using proprietary FacilityIE in the MGCP PRI Setup, Alert, and Connect messages.
- Unified Communications Manager plays the secure indication tone only to the Cisco Unified IP Phone. A PBX in the network plays the tone to the gateway end of the call.
- If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway is not encrypted, the call drops.

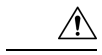
Note For more information about encryption for MGCP gateways, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for the version of Cisco IOS software that you are using.

H.323 Gateway and H.323/H.225/H.245 Trunk Encryption

H.323 gateways and gatekeeper or non-gatekeeper controlled H.225/H.323/H.245 trunks that support security can authenticate to Unified Communications Manager if you configure an IPSec association in the Cisco Unified Communications Operating System. For information on creating an IPSec association between Unified Communications Manager and these devices, refer to the *Administration Guide for Cisco Unified Communications Manager* .

The H.323, H.225, and H.245 devices generate the encryption keys. These keys get sent to Unified Communications Manager through the signaling path, which you secure through IPSec. Although Unified Communications Manager does not recognize whether an IPSec connection exists, the session keys get sent in the clear if IPSec is not configured. Confirm that the IPSec connection exists, so the session keys get sent through a secure connection.

In addition to configuring an IPSec association, you must check the SRTP Allowed check box in the device configuration window in Unified Communications Manager Administration; for example, the H.323 Gateway, the H.225 Trunk (Gatekeeper Controlled), the Inter-Cluster Trunk (Gatekeeper Controlled), and the Inter-Cluster Trunk (Non-Gatekeeper Controlled) configuration windows. If you do not check this check box, Unified Communications Manager uses RTP to communicate with the device. If you check the check box, Unified Communications Manager allows secure and nonsecure calls to occur, depending on whether SRTP is configured for the device.



Caution If you check the SRTP Allowed check box in Unified Communications Manager Administration, Cisco strongly recommends that you configure IPSec, so security-related information does not get sent in the clear.

Unified Communications Manager does not confirm that you configured the IPSec connection correctly. If you do not configure the connection correctly, security-related information may get sent in the clear.

If the system can establish a secure media or signaling path and if the devices support SRTP, the system uses a SRTP connection. If the system cannot establish a secure media or signaling path or if at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback (and vice versa) may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

Tip If the call uses pass-through capable MTP, if the audio capabilities for the device match after region filtering, and if the MTP Required check box is not checked for any device, Unified Communications Manager classifies the call as secure. If the MTP Required check box is checked, Unified Communications Manager disables audio pass-through for the call and classifies the call as nonsecure. If no MTP is involved in the call, Unified Communications Manager may classify the call as encrypted, depending on the SRTP capabilities of the devices.

For SRTP-configured devices, Unified Communications Manager classifies a call as encrypted if the SRTP Allowed check box is checked for the device and if the SRTP capabilities for the devices are successfully negotiated for the call. If the preceding criteria are not met, Unified Communications Manager classifies the call as nonsecure. If the device is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

Unified Communications Manager classifies outbound faststart calls over a trunk or gateway as nonsecure. If you check the SRTP Allowed check box in Unified Communications Manager Administration, Unified Communications Manager disables the **Enable Outbound FastStart** check box.

Unified Communications Manager allows some types of gateways and trunks to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

To enable the passing through of H.235 data, check the **H.235 pass through allowed** check box in the configuration settings of the following trunks and gateways:

- H.225 Trunk
- ICT Gatekeeper Control
- ICT non-Gatekeeper Control
- H.323 Gateway

For information about configuring trunks and gateways, see the *Administration Guide for Cisco Unified Communications Manager* .

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.

Configure Trunk and Gateway SIP Security Task Flow

Complete the following task to configure Gateway and SIP security.

Procedure

	Command or Action	Purpose
Step 1	Set Up Secure Gateways and Trunks	Enable secure Gateways and Trunks for security.
Step 2	Set Up SIP Trunk Security Profile	Add, update, or copy a SIP trunk security profile.
Step 3	Apply SIP Trunk Security Profile	Enable a SIP trunk security profile to the trunk and apply security profile to a device .
Step 4	Synchronize SIP Trunk Security Profile with SIP Trunks	Synchronize SIP trunks with a SIP Trunk security profile.
Step 5	Allow SRTP Using Unified Communications Manager Administration	Configure the SRTP Allowed option for H.323 gateways and gatekeeper or non-gatekeeper controlled H.323/H.245/H.225 trunks or SIP trunks.

Set Up Secure Gateways and Trunks

Use this procedure in conjunction with the document, *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*, which provides information on how to configure your CiscoIOS MGCP gateways for security.

Procedure

Step 1 Verify that you have run the **utils ctl** command to set the cluster in mixed mode.

Step 2 Verify that you configured the phones for encryption.

Step 3 Configure IPSec.

Tip You may configure IPSec in the network infrastructure, or you may configure IPSec between Unified Communications Manager and the gateway or trunk. If you implement one method to set up IPSec, you do not need to implement the other method.

Step 4 For H.323 IOS gateways and intercluster trunks, check the **SRTP Allowed** check box in Unified Communications Manager.

The **SRTP Allowed** check box displays in the **Trunk Configuration** or **Gateway Configuration** window. For information on how to display these windows, refer to the trunk and gateway chapters in the Administration Guide for Cisco Unified Communications Manager.

Step 5 For SIP trunks, configure the SIP trunk security profile and apply it to the trunk(s), if you have not already done so. Also, be sure to check the **SRTP Allowed** check box in the **Device** > **Trunk** > **SIP Trunk Configuration** window.

Caution If you check the **SRTP Allowed** check box, we recommend that you use an encrypted TLS profile, so that keys and other security-related information does not get exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Step 6 Perform security-related configuration tasks on the gateway.

For more information, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*.

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:

a) 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.

b) 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.

c) To update an existing profile, locate and display the appropriate security profile as described in Find SIP Trunk Security Profile.

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 (<>).
Device Security Mode	From the drop-down list, choose one of the following options: • **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. **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). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. 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.
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 Unified Communications Manager and the trunk.

Setting	Description
Outgoing Transport Type	From the drop-down list, 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. **Note** You must use UDP as the outgoing transport type only when connecting SIP trunks between Unified Communications Manager systems and other application do not support TCP. Else, use TCP as the default option.
Enable Digest Authentication	Check this check box to enable digest authentication. If you check this check box, Unified Communications Manager 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. **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, 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.

Setting	Description
Secure Certificate Subject or Subject Alternate Name	This field applies if you configured TLS for the incoming and outgoing transport type. 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. You can enter up to 4096 characters in this field. **Tip** The subject name corresponds to the source connection TLS certificate. Ensure that 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.
Incoming Port	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. **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.
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. Unified Communications Manager 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, 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. **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.

Setting	Description
Accept Presence Subscription	If you want Unified Communications Manager 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 Unified Communications Manager 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.
Accept Unsolicited Notification	If you want Unified Communications Manager 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 Replaces Header	If you want Unified Communications Manager 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.
Transmit Security Status	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. Default: This box is not checked.

Setting	Description
SIP V.150 Outbound SDP Offer Filtering	From the drop-down list, select one of the following filter options: • **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.
SIP V.150 Outbound SDP Offer Filtering	From the drop-down list, select one of the following filter options: • **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. **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.

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**.

Allow SRTP Using Unified Communications Manager Administration

The SRTP Allowed check box displays in the following configuration windows in Unified Communications Manager:

- H.323 Gateway Configuration window
- H.225 Trunk (Gatekeeper Controlled) Configuration window
- Inter-Cluster Trunk (Gatekeeper Controlled) Configuration window

- Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration window
- SIP Trunk Configuration window

To configure the SRTP Allowed check box for H.323 gateways and gatekeeper or non-gatekeeper controlled H.323/H.245/H.225 trunks or SIP trunks, perform the following procedure:

Procedure

Step 1 Find the gateway or trunk, as described in the Unified Communications Manager.

Step 2 After you open the configuration window for the gateway/trunk, check the **SRTP Allowed** check box.

Caution If you check the **SRTP Allowed** check box for a SIP trunk, we recommend that you use an encrypted TLS profile, so keys and other security-related information are not exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Step 3 Click **Save**.

Step 4 To reset the device, click **Reset**.

Step 5 Verify that you configured IPSec correctly for H323. (For SIP, make sure you configured TLS correctly.)