Configure SIP Trunks

- SIP Trunk Overview, on page 1
- SIP Trunk Configuration Prerequisites, on page 3
- SIP Trunk Configuration Task Flow, on page 3

SIP Trunk Overview

If you are deploying SIP for call control signaling, configure SIP trunks that connect Cisco Unified Communications Manager to external devices such as SIP gateways, SIP Proxy Servers, Unified Communications applications, remote clusters, or a Session Management Edition.

Within Cisco Unified CM Administration, the SIP Trunk Configuration window contains the SIP signaling configurations that Cisco Unified Communications Manager uses to manage SIP calls.

You can assign up to 16 different destination addresses for a SIP trunk, using IPv4 or IPv6 addressing, fully qualified domain names, or you can use a single DNS SRV record.

You can configure the following features on SIP trunks:

- Line and Name Identification Services
- Delayed Offer, Early Offer and Best Effort Early Offer
- Signaling encryption and authentication
- Media encryption with SRTP
- IPv6 dual stack support
- Video
- Presentation sharing with BFCP
- Far end camera control
- DTMF relay
- Calling party normalization
- URI dialing
- Q.SIG support
• T.38 fax support
• SIP OPTIONS
• Choice of DTMF signaling

Note
When Q.SIG is enabled in Small-scale IP telephony (SIPT) from Cluster A to Cluster B, and if "INVITE" is received with anonymous or any text, then the Cisco Unified Communications Manager does not encode it to Q.SIG data. When you decode the same in the leaf cluster, it displays empty and empty number is forwarded.

Note
When Q.SIG is enabled, URI dialing does not respond as expected and if Q.SIG is disabled, then the Cisco Call Back does not respond between two clusters.

IPv6 Dual Stack Support
You can also configure your SIP trunks with IPv6 dual stack support by configuring the IP Addressing Mode in a Common Device Configuration and then applying that configuration to the SIP trunk.

Note
You can also configure IPv6 clusterwide via a clusterwide service parameter. However, the Common Device Configuration setting overrides the clusterwide defaults.

Secure SIP Trunks
You can also configure your trunks with security such as digest authentication and signaling and media encryption by configuring a SIP trunk security profile that includes security features such as digest authentication and TLS signaling and associate that profile to the SIP trunks in your network. For the trunk to allow encrypted media, you must also configure the trunk to allow SRTP media.

SIP Trunk Security Profile Overview
You must assign a SIP trunk security profile to each SIP trunk in your network. By default, Cisco Unified Communications Manager applies a predefined, nonsecure SIP trunk security profile for autoregistration to all SIP trunks.

The SIP trunk security profile allows you to configure security settings such as digest authentication and TLS signaling encryption for the SIP trunks in your network. When you configure a SIP trunk security profile, and then assign that profile to a SIP trunk, the security settings from the profile get applied to the trunk.

You can configure multiple SIP trunk security profiles to cover the different security requirements that you have for different sets of SIP trunks in your network.

Note
To configure your network with security, you must also set up a CTL client and configure IPSec. For details, see the Security Guide for Cisco Unified Communications Manager.
SIP Trunk Configuration Prerequisites

Before you configure your SIP trunks, do the following:

- Plan your network topology so that you understand your trunk connections.
- Make sure that you understand the devices to which you want to connect your trunks and how those devices implement SIP. If those devices implement SIP, you may need to apply a SIP normalization script.
- Configure SIP profiles for your trunks.

In addition, configure the following before you configure your SIP trunks:
- SIP Normalization and Transparency Configuration Task Flow
- Configure SIP Profiles

SIP Trunk Configuration Task Flow

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure SIP Trunk Security Profile, on page 4</td>
<td>Configure SIP trunk security profiles with any security settings that you want to apply to your SIP trunks. For example, you can configure digest authentication, device security mode, and TLS encryption for SIP signaling. If you don't configure SIP trunk security profiles, by default, Cisco Unified Communications Manager applies a nonsecure sip trunk security profile.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure Common Device Configuration, on page 4</td>
<td>Set up a Common Device Configuration for the trunk. For dual-stack trunks, configure the IP addressing preference.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure SIP Trunks, on page 5</td>
<td>Configure the SIP trunks in your network. In the Trunk Configuration window, configure the SIP settings for your trunks. Assign a SIP profile, SIP trunk security profile, and a Common Device Configuration to your SIP trunk. In addition, assign any SIP normalization or transparency scripts that your trunk connection requires. For example, if your SIP trunk connects to a Cisco TelePresence VCS, you must assign the vcs-interop script to the SIP trunk.</td>
</tr>
</tbody>
</table>
Configure SIP Trunk Security Profile

Configure a SIP Trunk Security Profile with security settings such as digest authentication or TLS signaling encryption. When you assign the profile to a SIP trunk, the trunk takes on the settings of the security profile.

Note
If you don't assign a SIP trunk security profile to your SIP trunks, Cisco Unified Communications Manager assigns a nonsecure profile by default.

Procedure

Step 1 From Cisco Unified CM Administration, choose System > Security > SIP Trunk Security Profile.
Step 2 Click Add New.
Step 3 To enable SIP signaling encryption with TLS, perform the following:
   a) From the Device Security Mode drop-down list, select Encrypted.
   b) From the Incoming Transport Type and Outgoing Transport Type drop-down lists, choose TLS.
   c) For device authentication, in the X.509 Subject Name field, enter the subject name of the X.509 certificate.
   d) In the Incoming Port field, enter the port on which you want to receive TLS requests. The default for TLS is 5061.
Step 4 To enable digest authentication, do the following
   a) Check the Enable Digest Authentication check box
   b) Enter a Nonce Validity Timer value to indicate the number of seconds that must pass before the system generates a new nonce. The default is 600 (10 minutes).
   c) To enable digest authentication for applications, check the Enable Application Level Authorization check box.
Step 5 Complete the additional fields in the SIP Trunk Security Profile Configuration window. For more information on the fields and their configuration options, see Online Help.
Step 6 Click Save.

Note You must assign the profile to a trunk in the Trunk Configuration window so that the trunk can uses the settings.

Configure Common Device Configuration

A common device configuration comprises a set of optional set of user-specific feature attributes. If you are deploying IPv6, you can use this configuration to assign IPv6 preferences for SIP trunks or SCCP phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose Device > Device Settings > Common Device Configuration.
Step 2 Click Add New.
Step 3 For SIP trunks, SIP Phones or SCCP phones, choose a value for the IP Addressing Mode drop-down list:
Configure SIP Trunks

Use this procedure to configure a SIP trunk. You can assign up to 16 destination addresses for a SIP trunk.

Procedure

Step 1  From Cisco Unified CM Administration, choose Device > Trunk.
Step 2  Click Add New.
Step 3  From the Trunk Type drop-down list, choose SIP Trunk.
Step 4  From the Protocol Type drop-down list, choose the type of SIP trunk that matches your deployment and click Next:
   • None (Default)
   • Call Control Discovery
   • Extension Mobility Cross Cluster
   • Cisco Intercompany Media Engine
   • IP Multimedia System Service Control
Step 5  (Optional) If you want to apply a Common Device Configuration to this trunk, select the configuration from the drop-down list.
Step 6  Check the SRTP Allowed check box if you want to allow encrypted media over the trunk.
Step 7  Check the Run on All Active Unified CM Nodes check box if you want to enable the trunk for all cluster nodes.
Step 8  Configure the destination address for the SIP trunk:
   a) In the Destination Address text box, enter an IPv4 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.
b) If the trunk is a dual stack trunk, in the **Destination Address IPv6** text box, enter an IPv6 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.

c) If the destination is a DNS SRV record, check the **Destination Address is an SRV** check box.

d) To add additional destinations, click the (+).

**Step 9** From the **SIP Trunk Security Profile** drop-down, assign a security profile. If you don't select this option, a nonsecure profile will be assigned.

**Step 10** From the **SIP Profile** drop-down list, assign a SIP profile.

**Step 11** (Optional) If you want to assign a normalization script to this SIP trunk, from the **Normalization Script** drop-down list, select the script that you want to assign.

**Step 12** Configure any additional fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

**Step 13** Click **Save**.