Configure Trunks

SIP Trunk Overview

If you are deploying SIP for call control signaling, configure SIP trunks to connect Cisco Unified Communications Manager to external devices such as SIP gateways, SIP Proxy Servers, Unified Communications applications, conference bridges, 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 a single DNS SRV record.

SIP Trunk 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.
- Make sure that you have a device pool configured for the trunk.
- If you are deploying IPv6 on the trunk, you must configure the trunk's Addressing Preference via a clusterwide enterprise parameter or via a Common Device Configuration that you can apply to the trunk.
- If there are SIP interoperability issues with the applications that use the trunk, you may need to use one of the default SIP Normalization or Transparency scripts. If none of the default scripts meet your needs,

you can create your own script. For details on creating customized SIP Normalization and Transparency scripts, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

SIP Trunk Configuration Task Flow

Complete these tasks to set up your SIP trunks.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profiles, on page 2	Configure common SIP settings that you will apply to your SIP trunks.
Step 2	Configure SIP Trunk Security Profile, on page 3	Configure a security profile with security settings such as TLS signaling or digest authentication.
Step 3	Configure SIP Trunks, on page 3	Set up a SIP trunk and apply the SIP Profile and security profile to the trunk.

Configure SIP Profiles

Use this procedure to configure a SIP profile with common SIP settings that you can assign to SIP devices and trunks that use this profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Perform one of the following steps:

- Click **Find** and select the SIP profile to edit an existing profile, .
- Click **Add New** to create a new profile.

Step 3 If you want your SIP phones and trunks to support IPv4 and IPv6 stacks, check the **Enable ANAT** check box.

Step 4 If you want to assign an SDP transparency profile to resolve SDP interoperability, from the **SDP Transparency Profile** drop-down list.

Step 5 If you want to assign a normalization or transparency script to resolve SIP interoperability issues, from the **Normalization Script** drop-down list, select the script.

Step 6 (Optional) Check the **Send ILS Learned Destination Route String** check box for Global Dial Plan Replication deployments where you may need to route calls across a Cisco Unified Border Element.

Step 7 Complete the remaining fields in the **SIP Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

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 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 encypted 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**.

SIP Trunk Interactions and Restrictions

Feature	Description
Multiple Secure SIP Trunks to Same Destination	As of Release 12.5(1), Cisco Unified Communications Manager supports the configuration of multiple secure SIP trunks to the same Destination IP Address and Destination Port Number. This capability provides the following benefits: • Bandwidth optimization—Provides a route for emergency calls with unrestricted bandwidth • Selective routing based on a particular region or calling search space configuration

Feature	Description
Multiple Non-secure SIP Trunks to Same Destination	When multiple non-secure SIP trunks with different listening ports point to the same destination or port, they may incorrectly use the port in the mid call INVITE. Hence, the call drops.
Unified Communications Manager sends SIP-UPDATE message when it receives SIP 180 Ringing	The sip trunk sends an "UPDATE" SIP message when it receives "180 Ringing" after "183 Session Progress", provided the "UPDATE" value is supported in the call flow.
Presentation Sharing using BFCP	If you are deploying Presentation Sharing for Cisco endpoints, make sure that the **Allow Presentation Sharing with BFCP** check box is checked in the SIP Profile of all intermediate SIP trunks. **Note** For third-party SIP endpoints, you must also make sure that the same check box is checked within the **Phone Configuration** window.
iX Channel	If you are deploying iX Media Channel, make sure that the **Allow iX Application Media** check box is checked in the SIP Profiles that are used by all intermediate SIP trunks. **Note** For information on encrypted iX Channel, see the *Security Guide for Cisco Unified Communications Manager*.
90-day Evaluation License	You cannot deploy a secure SIP trunk while running with a 90-day evaluation period. To deploy a secure SIP trunk, your system must have registered to a Smart Software Manager account with the **Allow export-controlled functionality** product registration token selected.

H.323 Trunk Overview

If you have an H.323 deployment, H.323 trunks provide connectivity to remote clusters and other H.323 devices, such as gateways. H.323 trunks support most of the audio and video codecs that Unified Communications Manager supports for intracluster communications, except for wideband audio and wideband video. H.323 trunks use the H.225 protocol for call control signaling and the H.245 protocol for media signaling.

Within Cisco Unified CM Administration, H.323 trunks can be configured using the intercluster trunk (Non-Gatekeeper Controlled) trunk type and protocol options.

If you have a non-gatekeeper H.323 deployment, you must configure a separate intercluster trunk for each device pool in the remote cluster that the local Unified Communications Manager can call over the IP WAN. The intercluster trunks statically specify either the IPv4 addresses or hostnames of the remote devices.

You can configure up to 16 destination addresses for a single trunk.

Intercluster Trunks

When configuring intercluster trunk connections between two remote clusters, you must configure an intercluster trunk on each cluster and match the trunk configurations so that the destination addresses used by one trunk match the call processing nodes that are used by the trunk from the remote cluster. For example:

- Remote cluster trunk uses Run on all Active Nodes—The remote cluster trunk uses all nodes for call processing and load balancing. In the local intercluster trunk that originates in the local cluster, add in the IP addresses or hostnames for each server in the remote cluster.
- Remote cluster does not use Run on all Active Nodes—The remote cluster trunk uses the servers from the Unified Communications Manager Group that is assigned to the trunk's device pool for call processing and load balancing. In the local intercluster trunk configuration, you must add the IP address or hostname of each node from the Unified Communications Manager group that is used by the remote cluster trunk's device pool.

Secure Trunks

To configure secure signaling for H.323 trunks, you must configure IPSec on the trunk. For details, see the *Security Guide for Cisco Unified Communications Manager*. To configure the trunk to allow media encryption, check that the SRTP allowed check box in the **Trunk Configuration** window.

Note Gatekeepers are no longer widely used, but you can also configure your H.323 deployment to use gatekeeper-controlled trunks. For details on how to set up gatekeeper-controlled trunks, see *Cisco Unified Communications Manager Administration Guide*, Release 10.0(1).

H.323 Trunk Prerequisites

Plan out your H.323 deployment topology. For intercluster trunks, make sure you know which servers the corresponding remote cluster trunks use for call processing and load balancing. You will have to configure your local intercluster trunk to connect to each call processing server used by the trunk in the remote cluster.

If you are using Cisco Unified Communications Manager groups assigned to a trunk device pool for load balancing on the trunk, complete the configurations in Core Settings for Device Pools Configuration Task Flow section.

Configure H.323 Trunks

Use this procedure to configure trunks for an H.323 deployment.

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 box, choose **Inter-Cluster Trunk (Non-Gatekeeper Controlled)**.

Step 4 From the **Protocol** drop-down list box, choose **Inter-Cluster Trunk**.

Step 5 In the **Device Name** text box, enter the unique identifier for the trunk.

Step 6 From the **Device Pool** drop-down list box, select the device pool that you configured for this trunk.

Step 7 If you want to use every node in the local cluster for processing for this trunk, check the **Run on all Active Unified CM Nodes** check box.

Step 8 If you want to allow encrypted media across the trunk, check the **SRTP Allowed** check box.

Step 9 If you want to configure H.235 pass through, check the **H.235 Pass Through Allowed** check box.

Step 10 In the **Remote Cisco Unified Communications Manager Information** section, enter an IP address or hostname for each remote server to which this trunk connects.