Configure Third-Party SIP Phones

Third-Party SIP Endpoints Overview

In addition to the Cisco IP Phones that run SIP, Unified Communications Manager supports a variety of third-party SIP endpoints. You can configure the following third-party SIP endpoints in Cisco Unified Communications Manager Administration:

- Third-Party SIP Device (Advanced)— This eight-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies.
- Third-Party SIP Device (Basic)— This one-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies.
- Third-Party AS-SIP Device — Assured Services SIP (AS-SIP) endpoints are SIP endpoints compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides multiple endpoint interfaces on the Unified Communications Manager.
- Generic Desktop Video Endpoint —This SIP device supports video, security, configurable trust, and Cisco extensions. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.
- Generic Single Screen Room System —This SIP device supports single screen telepresence (room systems), video, security, configurable trust, and Cisco extensions. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.
- Generic Multiple Screen Room System — This SIP device supports multiple screen telepresence (room systems), video, security, configurable trust, and Cisco extensions. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.

Third-Party SIP Endpoints Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Digest User, on page 2	To enable digest authentication, configure an end user that is a digest user. Cisco Unified

	Command or Action	Purpose
		Communications Manager uses the digest credentials that you specify in the **End User Configuration** window to validate the SIP user agent response during a challenge to the SIP trunk. If the third-party SIP phone does not support a digest user, create a user with a user ID that matches the directory number of the third-party SIP phone. For example, create an end user named 1000 and create a directory number of 1000 for the phone. Assign this user to the phone.
Step 2	Configure SIP Profile	Provide a set of SIP attributes that are associated with SIP trunks.
Step 3	Configure Phone Security Profile, on page 3	To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication.
Step 4	Add a Third-Party SIP Endpoint, on page 4	Configure a third-party endpoint.
Step 5	Associate Device to End User, on page 5	Associate the third-party endpoint with an end user.

What to do next

Provide power, verify network connectivity, and configure network settings for the third-party SIP endpoint. For more information about configuring network settings, see the user guide for your third-party SIP endpoint.

Configure a Digest User

Perform these steps to configure an end user as a digest user. Digest authentication allows Cisco Unified Communications Manager to challenge the identity of a device that is connecting to Cisco Unified Communications Manager. When challenged, the device presents its digest credentials, similar to a username and password, to Cisco Unified Communications Manager for verification. If the credentials that are presented match those that are configured in the database for that device, digest authentication succeeds, and Cisco Unified Communications Manager processes the SIP request.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter a **User ID**.

Step 4 Enter a **Last Name**.

Step 5 Enter **Digest Credentials**. The digest credentials are a string of alphanumeric characters.

Step 6 Complete any remaining fields in the **End User Configuration** window. See the online help for more information about the fields and their configuration options..

Step 7 Click **Save**.

What to do next

Configure SIP Phone Secure Port

Configure SIP Profile

Use this procedure to configure SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks.

Before you begin

- Configure SIP Phone Secure Port
- Restart Services

Procedure

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

Step 2 Click **Find**.

Step 3 For the profile that you want to copy, click the file icon in the **Copy** column.

Step 4 Enter the name and description of the new profile.

Step 5 If you have the IPv6 stack configured and you are deploying two stacks, check the **Enable ANAT** check box.

Note This configuration applies whether you have Unity Connection deployed or not.

Step 6 Click **Save**.

What to do next

Configure Phone Security Profile, on page 3

Configure Phone Security Profile

Cisco Unified Communications Manager provides a set of predefined, nonsecure profiles for autoregistration. If you want to enable security features for a phone, you must configure a new security profile and apply it to the phone. Follow these steps to configure a new security profile:

Before you begin

If you are configuring SIP phones, complete the following procedures:

- Configure SIP Phone Secure Port
- Restart Services
- Configure SIP Profile

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Click **Add New**.

Step 3 From the **Phone Security Profile Type** drop-down list, choose the Universal Device Template to create a profile that you can use when provisioning through the device templates.

Note Optionally, you can also create security profiles for specific device models.

Step 4 Select the protocol.

Step 5 Enter an appropriate name for the profile in the **Name** field.

Step 6 If you want to use TLS signaling to connect to the device, set the **Device Security Mode** to **Authenticated** or **Encrypted** and the Transport Type to **TLS**.

Step 7 (Optional) Check the **Enable OAuth Authentication** check box if you want the phone to use digest authentication.

Step 8 (Optional) Check the **TFTP Encrypted Config** check box if you want to use encrypted TFTP.

Step 9 Complete the remaining fields in the Phone Security Profile Configuration window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

Add a Third-Party SIP Endpoint

Before you begin

Configure a Digest User, on page 2

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new third-party endpoint.
- Click **Find** to search and select an existing third-party endpoint.

Step 3 From the **Phone Type** drop-down list, choose one of the following:

- Third-party SIP Device (Basic)
- Third-party SIP Device (Advanced)

- Third-Party AS-SIP Device
- Third-party AS-SIP Endpoint
- Generic Desktop Video Endpoint
- Generic Single Screen Room System
- Generic Multiple Screen Room System

Step 4 From the **Digest User** drop-down list, choose the user that you created.

Step 5 Configure the fields in the **Phone Configuration** window. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 To configure a directory number for the third-party endpoint, click the **Add a New DN** link that displays in the **Association Information** area on the left side of the window.
The **Directory Number Configuration** window appears.

Step 8 Configure the fields in the Directory Number Configuration window. For help with the fields and their settings, see the online help.

What to do next

Associate Device to End User, on page 5

Associate Device to End User

Use this procedure to associate an end user to the third-party endpoint.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Find** and select the user whom you want to associate to the device.

Step 3 In the **Device Information** section, click **Device Association** .
The User Device Association window appears.

Step 4 Click **Find** to view a list of available devices.

Step 5 Select the device that you want to associate, and click **Save Selected/Changes**.

Step 6 From **Related Links**, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Third-Party Interactions and Restrictions

Third-Party Restrictions

Table 1: Third-Party SIP Endpoints Restrictions

Restriction	Description
Ringback tone restriction for Cisco Video Communications Server (VCS) registered to third-party SIP Endpoints	Blind transfer or switch to request the transfer which occurs over VCS registered endpoints with Cisco Unified Communications Manager will not have a ringback tone. If you do a supervised transfer, then you allocate Music On Hold (MOH) but, not a ringback tone.