Configure AS-SIP Endpoints

AS-SIP Overview

Assured Services SIP (AS-SIP) endpoints are compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides for multiple endpoint interfaces on the Unified Communications Manager.

Many Cisco IP phones support AS-SIP. In addition, the Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP compliant endpoint to be configured and used with Cisco Unified Communications Manager. In addition, the Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP-compliant generic endpoint to be configured and used with Cisco Unified Communications Manager

AS-SIP Capabilities

The following capabilities are implemented or made available for AS-SIP endpoints:

- MLPP
- TLS
- SRTP
- DSCP for precedence levels
- Error responses
- V.150.1 MER
- Conference Factory flow support
- AS-SIP Line Early Offer

Third-Party AS-SIP Phones

Third-party phones can be provisioned in Cisoc Unified Communications Manager using the Third-Party AS-SIP Endpoint device type.

Third-party phones that are running AS-SIP do not get configured through the Cisco Unified Communications Manager TFTP server. The customer must configure them by using the native phone configuration mechanism (usually a web page or TFTP file). The customer must keep the device and line configuration in the Cisco Unified Communications Manager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Cisco Unified Communications Manager). Also, if the directory number of a line is changed, the customer must ensure that it gets changed in both Cisco Unified CM Administration and in the native phone configuration mechanism.

Identification of Third-Party Phones

The third-party phones that are running SIP do not send a MAC address, they must identify themselves by using username. The REGISTER message includes the following header:

```
Authorization: Digest
username="swhite",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5",uri
="sip:172.18.197.224",
algorithm=MD5,response="126c0643a4923359ab59d4f53494552e"
```

The username, **swhite**, must match a user that is configured in the **End User Configuration** window of Cisco Unified CM Administration. The administrator configures the SIP third-party phone with the user; for example, **swhite**, in the **Digest User** field of **Phone Configuration** window.

Note You can assign each user ID to only one third-party phone. If the same user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Configuration of Third Party AS-SIP Phones and Cisco IP Phones

The following table provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running AS-SIP.

Table 1: Comparison of the Configuration Differences Between Cisco IP Phones and Third-Party Phones

Phone Running AS-SIP	Integrated with Centralized TFTP	Sends MAC Address	Downloads Softkey File	Downloads Dial Plan File	Supports Unified Communications Manager Failover and Fallback	Supports Reset and Restart
Cisco IP Phone	Yes	Yes	Yes	Yes	Yes	Yes
Third-party AS-SIP device	No	No	No	No	No	No

Note Not all Cisco IP Phones support AS-SIP. See the phone administration guide for your phone model for support information

Use Cisco Unified CM Administration to configure third-party phones that are running SIP (For more information, see "Configure SIP Profile" topic in *System Configuration Guide for Cisco Unified Communications Manager*

the). The administrator must perform configuration steps on the third-party phone that is running SIP; see the following examples:

- Ensure that proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Cisco Unified Communications Manager.
- Ensure directory numbers in the phone match the directory numbers that are configured for the device in Cisco Unified CM Administration.
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in the Cisco Unified CM Administration.

For more information, refer to the documentation that came with the third-party phone.

AS-SIP Conferencing

MOH is applied to its target (a held party, transferee just before transfer, or conferee just before joining the conference), if the feature invoker (holder, transferor, or conference initiator) supports Cisco-proprietary feature signaling. If the feature invoker does not support Cisco-proprietary feature signaling, then MOH is not applied to its target. Also, if an endpoint explicitly signals that it is a conference mixer, then MOH will not be played to the target. There are two forms of AS-SIP Conferencing:

- Local mixing
- Conference Factory

Local mixing

To the Unified CM, the conference initiator simply appears to have established simultaneously active calls, one to each of the other conference attendees. The initiator host the conference locally and the voices are mixed there. The calls from the conference initiator have special signaling that prevent it from being connected to an MOH source.

Conference Factory

The conference initiator calls a Conference Factory Server located off a SIP trunk. Through IVR signaling, the conference initiator instructs the Conference Factory to reserve a conference bridge. The Conference Factory gives the numeric address (a routable DN) to the conference initiator, who then establishes a subscription with the bridge to receive conference list information to track the participants. The Conference Factory sends special signaling that prevent it from being connected to an MOH Source.

AS-SIP Prerequisites

Determine whether sufficient Device License Units are available. For more information, see"Smart Software Licensing" chapter from *System Configuration Guide for Cisco Unified Communications Manager*

AS-SIP Enpdoint Configuration Task Flow

Complete the following tasks to configure an AS-SIP endpoint.

Procedure

	Command or Action	Purpose
Step 1	Configure a Digest User, on page 4	Configure the end user to use digest authentication for SIP requests.
Step 2	Configure SIP Phone Secure Port, on page 5	Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.
Step 3	Restart Services, on page 5	After configuring the secure port, restart the Cisco CallManager and Cisco CTL Provider services.
Step 4	Configure SIP Profile for AS-SIP, on page 6	Configure a SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks. **Note** The phone-specific parameters are not downloaded to a third-party AS-SIP phone. They are used only by Cisco Unified Communications Manager. Third-party phones must locally configure the same settings.
Step 5	Configure Phone Security Profile for AS-SIP, on page 6	You can use the phone security profile to assign security settings such as TLS, SRTP, and digest authentication
Step 6	Configure AS-SIP Endpoint, on page 7	Configure a Cisco IP Phone or a third-party endpoint with AS-SIP support.
Step 7	Associate Device with End User, on page 8	Associate the endpoint with a user.
Step 8	Configure SIP Trunk Security Profile for AS-SIP, on page 8	You can use the sip trunk security profile to assign security features such as TLS or digest authentication to a SIP trunk.
Step 9	Configure SIP Trunk for AS-SIP, on page 8	Configure a SIP trunk with AS-SIP support.
Step 10	Configure AS-SIP Features, on page 9	Configure additional AS-SIP features such as MLPP, TLS, V.150 and IPv6.

Configure a Digest User

Use this procedure to configure an end user as a digest user whom uses digest authentication. Devices that are associated to the user will be authenticated via the user's digest credentials.

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

Step 2 Do either of the following:

- Click **Add New** to create a new user.
- Click **Find** and select an existing user.

Step 3 Make sure the following mandatory fields are completed:

- User ID
- Last Name

Step 4 In the **Digest Credentials** field, enter a password. End users must authenticate themselves via this password when using the endpoint.

Step 5 Complete any remaining fields. For help with the fields and their settings, see the online help.

Step 6 Click **Save**.

Configure SIP Phone Secure Port

Follow these steps to configure the SIP Phone Secure Port. Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.

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

Step 2 In the **Cisco Unified Communications Manager TCP Port Settings for this Server** section, specify a port number in the **SIP Phone Secure Port** field, or leave the field set to default. The default value is 5061.

Step 3 Click **Save**.

Step 4 Click **Apply Config**.

Step 5 Click **Ok**.

Restart Services

Follow these steps to restart Cisco CallManager and Cisco CTL Provider services.

Step 1 From the Cisco Unified Serviceability interface, choose **Tools** > **Control Center - Feature Services**.

Step 2 Choose the Cisco Unified Communications Manager server from the **Servers** drop-down list.
In the CM Services area, Cisco CallManager displays in the **Service Name** column.

Step 3 Click the radio button that corresponds to the Cisco CallManager service.

Step 4 Click **Restart**.
The service restarts and displays the message, `Service Successfully Restarted`.

Step 5 Repeat step 3 and step 4 to restart Cisco CTL Provider service.

Configure SIP Profile for AS-SIP

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

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

Step 2 Do either of the following:

- Click **Add New** to create a new SIP Profile.
- Click **Find** and select an existing SIP Profile.

Step 3 Enter a **Name** and **Description** for the SIP Profile.

Step 4 Check the **Assured Services SIP conformance** check box.

Note This checkbox must be checked for SIP trunks and for third-party AS-SIP phones. It's not mandatory for Cisco IP Phones that support AS-SIP.

Step 5 In the **Parameters used in Phone** section, configure DSCP precedence values for the types of calls that you expect to make.

Note You can also configure DSCP values via clusterwide service parameters. However, the DSCP values within a SIP Profile override the clusterwide settings for all devices that use the SIP Profile.

Step 6 From the **Early Offer support for voice and video calls** drop-down list, select one of the following options to configure Early Offer support for SIP trunks that use this profile:

- Disabled
- Best Effort (no MTP Inserted)
- Mandatory (insert MTP if needed)

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 Phone Security Profile for AS-SIP

Use this procedure to configure a phone security profile for AS-SIP endpoints. You can use the security profile to assign security settings such as TLS and SRTP.

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

Step 2 Perform one of the following steps:

- Click **Add New** to create a new phone security profile.
- Click **Find** to edit an existing profile.

Step 3 For new profiles, select an option from the **Phone Security Profile** drop-down, choose the phon emodel**Third-party AS-SIP Endpoint** and click **Next**.

- For Cisco IP phones, select the phone model and click **Next**.
- For third-party AS-SIP endpoints, select **Third-party AS-SIP Endpoint** and click **Next**.

Step 4 For the protocol, select **SIP** and click **Next**.

Step 5 Enter a **Name** and **Description** for the protocol.

Step 6 Assign the **Device Security Mode**, to one of the following settings:

- **Authenticated**—Cisco Unified Communications Manager uses TLS signaling, providing integrity and authentication for the phone.
- **Encrypted**—Cisco Unified Communications Manager uses TLS signaling, providing integrity and authentication for the phone. In addition, SRTP encrypts the media streams.

Step 7 Check the **Enable Digest Authentication** check box.

Step 8 Configure the remaining fields in the **Phone Security Profile Configuration** window. For help with the fields and their settings, see the online help.

Step 9 Click **Save**.

Configure AS-SIP Endpoint

Use this procedure to configure an AS-SIP endpoint. Many Cisco IP Phones support AS-SIP. In addition, you can configure AS-SIP for third-party endpoints.

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

Step 2 Click **Add New**.

Step 3 From the Phone Type drop-down list, select a Cisco IP Phone that supports AS-SIP. Otherwise, select **Third-Party AS-SIP Endpoint**.

Step 4 Click **Next**.

Step 5 Configure the following mandatory fields.For more information on the fields and their configuration options, see Online Help.

- Device Trust Mode—For third-party AS-SIP endpoints only. Select **Trusted** or **Not Trusted**.
- MAC Address
- Device Pool
- Phone Button Template
- Owner User ID
- Device Security Profile—Select the phone security profile that you set up for AS-SIP.
- SIP Profile—Select the AS-SIP-enabled SIP Profile that you configured.
- Digest User—Select the user ID that you configure as a digest user. The user must be enabled for digest authentication
- Require DTMF Reception—Check this check box to allow the endpoint to accept DTMF digits.
- Early Offer support for voice and video calls—Check this check box to enable early offer support. This field appears for third-party phones only.

Step 6 Configure the fields in the **MLPP and Confidential Access Level Information** section.

Step 7 Click **Save**.

Step 8 Add a Directory Number:

a) In the left navigation bar, click **Add a new DN**. The **Directory Number Configuration** window opens.
b) Add a **Directory Number**.
c) Complete any remaining fields in the **Directory Number Configuration** window
d) Click **Save**.

Step 9 From **Related Links**, select **Configure Device** and click **Go**.

Step 10 Click **Apply Config**.

Associate Device with End User

Use this procedure to associate an end user to the AS-SIP endpoint.

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.

Configure SIP Trunk Security Profile for AS-SIP

Use this procedure to configure a security profile for a SIP trunk that supports AS-SIP

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

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the security profile.

Step 4 From the **Device Security Mode** drop-down list, choose **Authenticated** or **Encrypted**.

Step 5 The **Incoming Transport Type** and **Outgoing Transport Type** fields change to **TLS** automatically.

Step 6 Check the **Enable Digest Authentication** check box.

Step 7 If you are deploying V.150, configure a value for the **SIP V.150 Outbound SDP Offer Filtering** drop-down list.

Step 8 Complete the remaining fields in the **SIP Trunk Security Profile Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 9 Click **Save**.

Configure SIP Trunk for AS-SIP

Use this procedure to set up a SIP trunk that supports AS-SIP.

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

Step 2 Do either of the following:

- Click **Find** and select an existing trunk.
- Click **Add New** to create a new trunk.

Step 3 For new trunks, from the **Trunk Type** drop-down list, select **SIP Trunk**.

Step 4 From the **Trunk Service Type** drop-down list, select **None (Default)** and click **Next**.

Step 5 Enter a **Device Name** for the trunk.

Step 6 From the **Device Pool** drop-down list, select a device pool.

Step 7 In the **Destination Address** field, enter the address of the server to which you are connecting the trunk.

Step 8 From the **SIP Trunk Security Profile** drop-down list, select the profile that you created for AS-SIP.

Step 9 From the **SIP Profile** drop-down list, select the SIP Profile that you set up for AS-SIP.

Step 10 Complete any remaining fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 11 Click **Save**.

Configure AS-SIP Features

The procedures in the preceding task flow describe how to configure AS-SIP support on endpoints and trunk. The following table outlines the AS-SIP features that you can deploy and provides configuration reference for each.

AS-SIP Feature	Configuration Description
Early Offer	SIP Early Offer allows your endpoints to negotiate media during the INVITE request and the 200OK response. There are two modes for Early Offer: • Best Effort Early Offer (no MTP Inserted) • Mandatory Early Offer (insert MTP if needed) Configure Early Offer support via the fields in the following configuration windows. Refer to the online help for detailed field descriptions: **SIP Profile Configuration** window • Early Offer support for voice and video calls—Configure this field to enable Early Offer support on a SIP trunk • SDP Session-level Bandwidth Modifier for Early Offer and Re-invite • Send send-receive SDP in mid-call INVITE **Phone Configuration** window (only if the Third Pary AS-SIP Endpoint device type is used) • Early Offer support for voice and video calls - check this check box to enable early offer support

AS-SIP Feature	Configuration Description
Conference Factory	Specify the URI that an IMS client uses to set up a conference: 1. From Cisco Unified CM Administration, choose **System** > **Service Parameters**. 2. From the **Server** drop-down list select your Cisco Unified Communications Manager server. 3. From the **Service**, select **Cisco CallManager**. 4. Under **Clusterwide Paramters (Feature - Conference)** assign an **IMS Conference Factory URI**. 5. Click **Save**.
DSCP Markings	DSCP settings allow you to manage QoS and bandwidth within your network. DSCP settings are used to assign a prioritized Traffic Class Label to calls on a per-call basis. You can configure clusterwide DSCP settings via service parameters and you can use the SIP Profile to assign a customized QoS policy for users whom use that profile. For example, you could assign higher priority for the calls of an executive (for example, a CEO) or a sales team to ensure that their calls are not dropped if network bandwidth issues arise. To configure DSCP, see DSCP Settings Configuration Task Flow.
IPv6	By default, Cisco Unified Communications Manager is configured to use IPv4 addressing. However, you can configure the system to support the IPv6 stack thereby allowing you to deploy a SIP network with IPv6-only endpoints. For more information to configure IPv6, see "Dual Stack IPv6 Configuration Task Flow" chapter in the *System Configuration Guide for Cisco Unified Communications Manager*
Multilevel Precedence and Preemption (MLPP)	The Multilevel Precedence and Preemption (MLPP) service allows placement of priority calls. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations. To configure MLPP, see Multilevel Precendence and Preemption Task Flow.
Secure Real-Time Transport Protocol (SRTP)	The Secure Real-time Transport Protocol (SRTP) can be used to provide encryption and authentication to media streams in your calls. SRTP can be configured for phones within the **Phone Security Profile Configuration** that the phone uses. You must set the **Device Security Mode** field to **Encrypted**.
Transport Layer Signalling (TLS)	Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. For more information to configure TLS, see the "TLS Setup" chapter in the *Security Guide for Cisco Unified Communications Manager*.

AS-SIP Feature	Configuration Description
V.150	The V.150 Minimum Essential Requirements feature allows you to make secure calls in a modem over IP network. The feature uses a dialup modem for large installed bases of modems and telephony devices operating on a traditional public switched telephone network (PSTN). For more information to configure V.150, see the "Cisco V.150 Minimum Essential Requirements (MER)" chapter in the *Security Guide for Cisco Unified Communications Manager*.