AS-SIP configuration

Assured Services SIP (AS-SIP) endpoints are SIP endpoints compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides for multiple endpoint interfaces on the Unified Communications Manager. The Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP-compliant generic endpoint to be configured and used with the Unified CM.

The Cisco-proprietary RoundTable (RT) 8961, 9951 and 9971 SIP phones, and their corresponding Unified CM interfaces, are enhanced to provide AS-SIP features. The RT MLPP behavior maintains feature parity with SCCP MLPP implementation. The SIP signaling interface between Unified CM and RT phones is different from the interface between Unified CM and Third-Party AS-SIP Endpoint. The Unified CM sends new configuration parameters to the RT endpoint as part of the extended mark-up language (XML) configuration file. These parameters enable and disable the AS-SIP features and also govern how the RT endpoint operates when using this functionality. The RT endpoint also parses, processes, and sends new headers indicating resource priority for a given call. The RoundTable enhancements focus on TFTP configuration and SIP call processing exchanges between the RT endpoint and the Unified CM.

AS-SIP capabilities

The following capabilities are implemented or made available for the Third-Party AS-SIP Endpoint interface in compliance with LSC and AS-SIP Line requirements:

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

Note With the exception of AS-SIP Line Early Offer, these capabilities were also implemented, made available, or already existed for the RT 8961, 9951 and 9971 phones and corresponding Unified CM interfaces, in compliance with LSC and SIP EI requirements.

Set up AS-SIP line endpoints

Unified CM supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. This procedure lists the tasks used to manually configure a third-party phone that is running SIP. Use Cisco Unified Communications Manager Administration to configure third party phones.

Procedure

Step 1 Gather the following information about the phone:

- Physical location of the phone Unified Communications Manager user to associate with the phone
- Partition, calling search space, and location information, if used
- Number of lines and associated DNs to assign to the phone

Step 2 Determine whether sufficient Device License Units are available.
All licensing for Unified CM and Unity Connection is centralized and held on the Enterprise License Manager. For more information, refer to the *Enterprise License Manager User Guide*.

Step 3 Configure the end user that will be the Digest User.
See topics related to End User configuration settings for field descriptions.

Note MLPP authentication (optional) requires the phone to send in an MLPP username and password. The end user specifies the highest MLPP precedence level allowed for that user. MLPP credentials are tied to the user while the need to use them is tied to the device (via the MLPP Authorization checkbox in the SIP Profile used by the device).

Step 4 Configure the SIP Profile or use the default profile. The SIP Profile gets added to the phone that is running SIP by using the **Phone Configuration** window.
Third-party AS-SIP phones use the SIP Profile Information section of the **SIP Configuration** window along with the following fields from the phone specific parameters section:

- Resource Priority Namespace
- MLPP User Authorization

Note The phone specific parameters are not downloaded to a third-party AS-SIP phone. They are only used by the Unified CM. Third party phones must locally configure the same settings.

See topics related to SIP profile configuration settings and configuring Cisco Unified IP Phones for more information.

Step 5 Configure the phone security profile.
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. See topics related to phone security profile configuration and the *Cisco Unified Communications Manager Security Guide* for more information.

The phone security profile must be configured for TLS. See “TLS” section for details.

Step 6 Add and configure the third-party phone that is running SIP by choosing Third-party AS-SIP Endpoint from the **Add a New Phone Configuration** window.
See topics related to configuring Cisco Unified IP Phones for more information.

Step 7 Add and configure lines (DNs) on the phone.
See topics related to directory number configuration for more information.

Step 8 In the **End User Configuration** window, associate the third-party phone that is running SIP with the user by using Device Association and choosing the phone that is running SIP.
See topics related to associating devices to an end user for more information.

Step 9 In the Digest User field of the **Phone Configuration** window, choose the end user that you created in Step 3.

Step 10 Provide power, install, verify network connectivity, and configure network settings for the third-party phone that is running SIP.
See the administration guide that was provided with your phone that is running SIP.

Step 11 Make calls with the third-party phone that is running AS-SIP.
See the user guide that came with your third-party phone that is running SIP.

Configuration differences for phones running AS-SIP

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.

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 Unified IP Phone 8961, 9951, 9971	Yes	Yes	Yes	Yes	Yes	Yes
Third-party AS-SIP device	No	No	No	No	No	No

Use Unified CM Administration to configure third-party phones that are running SIP (see the "SIP Profile Configuration Settings" section). The administrator must also perform configuration steps on the third-party phone that is running SIP; see following examples:

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

Consult the documentation that came with the third-party phone that is running SIP for more information.

AS-SIP conferencing

MOH is applied to its target (a held party, transferee just prior to transfer, or conferee just prior to 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 conference is hosted locally by the initiator 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 of 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 keep track of participants. The Conference factory sends special signaling that will prevent it from being connected to an MOH Source.

Unified Communications Manager identification of third-party phones

Because 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 an end user that is configured in the End User Configuration window of Unified CM Administration (see End User Configuration Settings). The administrator configures the SIP third-party phone with the user; for example, swhite, in the Digest User field of Phone Configuration window (see Configuring Cisco Unified IP Phones).

Note You can assign each end user ID to only one third-party phone (in the Digest User field of the Phone Configuration window). If the same end user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Third-party phones running AS-SIP

Third-party phones that are running AS-SIP do not get configured by using the Unified Communications Manager TFTP server. The customer configures 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 Unified Communications Manager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Unified Communications Manager). Additionally, if the directory number of a line is changed, ensure that it gets changed in both Unified CM Administration and in the native phone configuration mechanism.

End user configuration settings

The End User Configuration window in Unified CM Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window. If MLPP Authorization is enabled for AS-SIP, MLPP Authorization must also be configured on the End User administration page. This MLPP Authentication requires a user identification number and a password. The MLPP User Identification number must be composed of 6 - 20 numeric characters and the MLPP Password must be composed of 4 - 20 numeric

characters. The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override.

Note Extension Mobility is not supported for third-party AS-SIP devices.

Note Third-party AS-SIP does not support CAPF.

SIP profile configuration settings

The SIP profile configuration settings contains an 'Is Assured SIP Service Enabled' checkbox. This should be checked for third-party AS-SIP endpoints, as well as AS-SIP trunks. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Enable digest authentication for third-party phones running SIP

To enable digest authentication for third-party phones that are running SIP, the administrator must create a Phone Security Profile. (See the "Phone Security Profile Configuration" section a general description and the Unified Communications Manager Security Guide for details.) On the Phone Security Profile Configuration window, check the Enable Digest Authentication check box. After the security profile is configured, the administrator must assign that security profile to the phone that is running SIP by using the Phone Configuration window. If this check box is not checked, Unified CM will use digest authentication for purposes of identifying the phone by the end user ID, and it will not verify the digest password. If the check box is checked, Unified CM will verify the password.

DTMF Reception

To require DTMF reception, check the Require DTMF Reception check box that displays on the Phone Configuration window in Unified CM Administration.

Phone Security Profile Configuration

In Unified CM Administration, use the **System > Security > Phone Security Profile** menu path to configure phone security profiles.

The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Unified CM Administration.

Require DTMF reception

Set up phone security profile settings

Set up TLS

For TLS for third-party AS-SIP devices, configure your call manager correctly using the procedures found in the Security chapter in the Unified Communications Operating System Administration Guide.

You will also need to follow your local procedures for generating certificates.

For information on configuring and applying a phone security profile, see the Unified Communications Manager Security Guide.

Add and configure third-party phones

Adding and configuring AS-SIP devices is virtually identical to existing third-party device types. There are, however, a few differences. The AS-SIP device type:

- Can be configured for MLPP
- Includes an optional Device Security Mode in the security profile
- For Third-party AS-SIP devices, the preemption setting is not available on the Unified CM. It is completely controlled by the third-party phone.
- Supports Early Offer for voice and video calls

Note Early Offer support for voice and video calls sends an SDP offer in the initial INVITE to the called party.

If Early Offer is enabled for a device, and the Unified CM expects to receive delayed offer calls, a Media Resource Group List must be configured in order to prevent the insertion of MTPs.

Use the following procedure to configure a media resource group list.

Procedure

Step 1 In CUCM Administration, choose **Media Resources > Media Resource Group**.

Step 2 Click the **Add New** button to add a new Media Resource Group List.

Step 3 In the Media Resource Group List, add only the Unified CM-based software MTPs to the Media Resource Group (MRG). Unified CM software resources are typically named MTP_# where # is a number (for example, "MTP_2").

Step 4 This media resource group, which should now contain all the software MTP resources from Unified CM, should not be applied to any media resource group list (MRGL). By placing the MTP resources in an MRG,

but not in an MRGL, these MTP resources are not be available to any of the devices on the system— which is the desired behavior.

Note If the system also has configured hardware MTP resources (which it does not by default), these must also be made unavailable using the same procedure.

For more information on adding and configuring third party phones, see Cisco Unified IP Phone Configuration, CUCM Administration Guide.