New and Changed Info for Cisco Unified Communications Manager Release 8.5(1)

New and Changed Information

This section contains information on the following topics:

- Installation, Upgrade, and Migration, page 1
- Command Line Interface, page 1
- Cisco Unified Communications Manager Administration, page 2
- Cisco Unified Communications Manager Features and Applications, page 5
- Security, page 44
- Bulk Administration Tool, page 48
- Cisco Unified IP Phones and Video Endpoints, page 50
- Cisco Unified Serviceability, page 62

Installation, Upgrade, and Migration

This section contains information on the following topics:

Command Line Interface

The following new CLIs exist for this release:

- **utils sso enable**—Refer to the "Single Sign On" section on page 26.
- **utils sso disable**—Refer to the "Single Sign On" section on page 26.
- **utils sso status**—Refer to the "Single Sign On" section on page 26.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

- New and Updated Enterprise and System Parameters, page 2
- Menu Changes, page 2

New and Updated Enterprise and System Parameters

The following sections contain information on new and updated enterprise and service parameters:

- Enterprise Parameters, page 2
- Service Parameters, page 2

Enterprise Parameters

No new or updated enterprise parameters exist in Cisco Unified Communications Manager 8.5(1).

Service Parameters

To access the service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**. Choose the server and the service name that the parameter supports. For some parameters, you may need to click Advanced to display the service parameter. To display the help for the service parameter, click the name of the service parameter in the window.

- Redial Await Timer (in Cisco - Mobility section)—Use this service parameter when you configure the Session Resumption feature.
- Allow Barge When Ringing (in Single Button Barge)—Use this service parameter to allow a user to barge into a call when the phone is ringing out or when the call is connected (the barger hears a ringback tone).

Menu Changes

This section contains information on the following menus in Cisco Unified Communications Manager Administration:

- Main Window, page 2
- System, page 3
- Call Routing, page 3
- Media Resources, page 3
- Voice Mail, page 3
- Device, page 3
- Application, page 4
- User Management, page 4
- Bulk Administration, page 4

Main Window

No changes exist for the main window.

System

The System menu contains the following updates:

- **System > Service Parameters**—See the "New and Updated Enterprise and System Parameters" section on page 2.

Call Routing

The Call Routing menu contains the following updates:

- **Call Routing > Mobility Configuration**—This menu option is removed in Release 8.5(1) of Cisco Unified Communications Manager Administration.
- **Call Routing > Mobility > Enterprise Feature Access Configuration**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See "Mobility Feature Enhancements" section on page 17 for details.)
- **Call Routing > Mobility > Handoff Configuration**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See "Mobility Feature Enhancements" section on page 17 for details.)
- **Call Routing > Mobility > Mobility Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See "Mobility Feature Enhancements" section on page 17 for details.)
- **Call Routing > Route/Hunt > Route List—**New check box Run On All Active Unified CM Nodes is added to the Route List Configuration page.

Media Resources

No changes exist for the Media Resources menu.

Voice Mail

No changes exist for the Voice Mail menu.

Device

The following changes exist for the Device menu:

- **Device > Device Settings > SIP Profile**—New fields were added to support the SIP OPTIONS feature (see SIP OPTIONS, page 34).
  - Enable OPTIONS Ping to monitor destination status for trunks with service type "None (Default)"
  - Ping Interval for In-service or Partially In-service Trunks (seconds)
  - Ping Interval for Out-of-service SIP Trunks (seconds)
  - Ping Retry Timer (milliseconds)
  - Ping Retry Count
  - Deliver Conference Bridge Identifier—This new check box supports the ORA SIP Enhancements for Call Recording feature. (See "SIP Header Enhancements for Call Recording" section on page 31 for details.)
- **Device > Trunk—**New check box Run On All Active Unified CM Nodes is added to the Trunk Configuration page.
- **Device > Trunk > SIP Trunk**—New fields and check boxes were added to support the QSIG Tunneling over SIP feature (see Q.SIG Tunneling over SIP, page 23).
  - Tunneled Protocol

  - QSIG Variant
  - ASN.1 ROSE OID Encoding
  - Path Replacement Support check box
  - Transmit UTF-8 Names in QSIG APDU check box
- **Device > Trunk > SIP Trunk**—New field, Consider Traffic on This Trunk Secure, was added to support SIP trunk security (see SIP Trunk Security Enhancements, page 25).
  - When using both sRTP and TLS
  - When using sRTP Only

Application

No updates or new fields exist for this menu.

User Management

No updates or new fields exist for this menu.

Bulk Administration

The Bulk Administration menu displays the following new and updated settings:

- **Bulk Administration > Users > End User CAPF Profile > Insert End User CAPF Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Inserting End User CAPF Profile, page 48.)
- **Bulk Administration > Users > End User CAPF Profile > Delete End User CAPF Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Deleting End User CAPF Profile, page 48.)
- **Bulk Administration > Users > End User CAPF Profile > Export End User CAPF Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Exporting End User CAPF Profile, page 49.)
- **Bulk Administration > User Device Profiles > Update UDP > Query**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Using Query to Update UDPs, page 49.)
- **Bulk Administration > User Device Profiles > Update UDP > Custom File**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Using Custom File to update UDPs, page 49.)
- **Bulk Administration > Mobility > Mobility Profile > Insert Mobility Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Inserting Mobility Profile, page 49.)
- **Bulk Administration > Mobility > Mobility Profile > Delete Mobility Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Deleting Mobility Profile, page 50)
- **Bulk Administration > Mobility > Mobility Profile > Export Mobility Profile**—This menu option is added in Release 8.5(1) of Cisco Unified Communications Manager Administration. (See Exporting Mobility Profile, page 50.)

Cisco Unified Communications Manager Features and Applications

This section contains information on the following Cisco Unified Communications Manager Administration features and applications:

- Agent Greeting, page 5
- Assisted Directed Call Park Support Enhancements, page 6
- Call Back No Answer Support for VG224, page 6
- Cisco Mobile 8.0 Support, page 6
- Cisco UCS C200 High-Density Rack-Mount Server Support, page 7
- Cisco UCS C210 Rack-Mount Server Support, page 7
- Cisco Unified Communications Manager Assistant Browser Changes, page 7
- Early Offer, page 7
- EMCC Device Maintains Network Setting, page 17
- Interoperability with Cisco Unified Customer Voice Portal Release 7.0(2), page 17
- IP Phone Service Enhancements, page 17
- Mobility Feature Enhancements, page 17
- Platform, page 23
- Q.SIG Tunneling over SIP, page 23
- SIP Trunk Security Enhancements, page 25
- Single Sign On, page 26
- SIP Header Enhancements for Call Recording, page 31
- SIP OPTIONS, page 34
- SIP Normalization and Transparency, page 38
- Static Routing Enhancements (Run Route List on all nodes), page 39
- Third-Party SIP Endpoints, page 40
- Video and Interoperability Enhancements, page 41
- Unified Communication OS Upgrade, page 44
- Whisper Coaching, page 44
- Windows 7 Support for RTMT, page 44

Agent Greeting

Agent Greeting allows an agent or administrator to create and play a prerecorded greeting automatically at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. An Agent can prerecord a single greeting or multiple ones as needed and create and update them. When a customer calls, both callers hear the prerecorded greeting. The agent can remain on mute until the greeting ends or answer the call over the greeting. All codecs supported for the phone are supported for Agent Greeting calls.

To enable Agent Greeting in the Cisco Unified Communications Manager Administration application, choose **Device > Phone**, locate the Cisco Unified IP Phone that you want to configure. Scroll to the Device Information Layout pane and set Built-in Bridge to **On** or **Default**. If Built-in Bridge is set to

Default, in the Cisco Unified Communications Manager Administration application, choose **System > Service Parameter** and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (**Device - Phone**) pane and set Built-in Bridge Enable to **On**.

For More Information

- Agent Greeting feature documentation, *CTI Product Description Guide for Cisco Unified Contact Center Enterprise, Release 8.5(1)*
- Features Supported by Cisco Unified JTAPI, *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager 8.5(1)*
- Features Supported by TSP, *Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager 8.5(1)*

Assisted Directed Call Park Support Enhancements

Cisco Unified Communications Manager 8.5(1) supports Assisted Directed Call Park on the Cisco Unified IP Phones 7900 Series (SIP).

Assisted directed call park is supported on all Cisco Unified IP Phones 7900, 8900, and 9900 series that support SIP. Assisted directed call park means that the end user needs to press only one button to direct-park a call. This requires you to configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call will be immediately parked at the Dpark slot associated with the Directed Call Park feature button.

Call Back No Answer Support for VG224

Cisco Unified Communications Manager Release 8.0 and earlier supported Call Back only on busy subscriber for Cisco VG224 endpoints. Cisco Unified Communications Manager Release 8.5 and later supports Call Back No Answer for Cisco VG224 endpoints.

For more information on the Call Back feature, see the *Cisco Unified Communications Manager Features and Services Guide*.

Cisco Mobile 8.0 Support

Cisco Unified Communications Manager supports SIP-based dual-mode mobile phones with Cisco Mobile 8.0. Cisco Unified Communications Manager supports the new Cisco Dual Mode for iPhone device type for iPhone, which specifies a SIP-based dual-mode mobile phone that is capable of leveraging VoIP connectivity over the enterprise WLAN.

Cisco Unified Communications Manager supports dual-mode mobile phones that use the Cisco Unified Mobile Communicator client and SIP protocol within the WLAN. Cisco Unified Communications Manager must handle dual SIP registrations (one from Cisco Unified Mobile Communicator via Cisco Unified Mobility Advantage and one from Wi-Fi as a SIP endpoint).

Cisco Mobile 8.0 provides iPhone users with voice over IP (VoIP) calling, visual voicemail, and access to the corporate directory while users are connected to the corporate network over Wi-Fi, either on premises or over VPN. Cisco Mobile 8.0 specifies an IP telephony endpoint that associates with Cisco Unified Communications Manager.

Note Cisco Mobile 8.0 is distinct from the Cisco Mobile application that runs in conjunction with a Cisco Unified Mobility Advantage server.

In order for Cisco Unified Communications Manager to support Cisco Mobile 8.0, Cisco Unified Communications Manager administrators must take at least the following step:

1. Configure the new device in Cisco Unified Communications Manager Administration.

Note Note that in Release 8.5(1) of Cisco Unified Communications Manager Administration, downloading of a COP file is not required.

The *Administration Guide for Cisco Mobile 8.0 for iPhone* provides the details of the complete configuration that is required to configure Cisco Mobile 8.0, including the steps that must be performed in Cisco Unified Communications Manager Administration. Refer to the document at the following URL:

http://www.cisco.com/en/US/products/ps7271/prod_installation_guides_list.html

Cisco UCS C200 High-Density Rack-Mount Server Support

Cisco Unified Communications Manager Releases 8.5(1) and later support the Cisco UCS C200 High-Density Rack-Mount Server. This server runs Cisco Unified Communications Manager through VMware ESXi only.

For more information, refer to this document's Platform section and to the Unified Communications Virtualization wiki at http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization.

Cisco UCS C210 Rack-Mount Server Support

Cisco Unified Communications Manager Releases 8.0(3) and later support the Cisco UCS C210 General-Purpose Rack-Mount Server, Reference Configurations 2 and 3. This server runs Cisco Unified Communications Manager through VMware ESXi only.

For more information, refer to this document's Platform section and to the Unified Communications Virtualization wiki at http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization.

Cisco Unified Communications Manager Assistant Browser Changes

Cisco Unified Communications Manager Assistant administration (using Cisco Unified Communications Manager Administration) and the Assistant Console are supported on Microsoft Internet Explorer (IE) 5.5 or later, Firefox 3.x or later, and Safari 4.x or later.

Early Offer

Description

To enhance interoperability with third party SIP devices, Cisco Unified Communications Manager now allows you to configure SIP trunks to enable early offer for outgoing voice and video calls without requiring MTP, when media capabilities and media port information of the calling endpoint is available. For outgoing call setup for an early offer trunk, Cisco Unified Communications Manager includes an SDP with the calling device media port, codecs, and IP address of the calling device (when available); inserts an MTP for early offer only when the media information for the caller is unavailable; and advertises multiple codecs when an MTP that supports multiple codecs gets inserted. In previous releases, Cisco Unified Communications Manager only provided early offer SDP when administrators enabled MTP Required or E2E RSVP on the outgoing SIP trunk. The early offer feature enhancement in

this release ensures that a higher percentage of outbound early offer SIP trunk calls get made without requiring an MTP, thus reducing the number of MTP resources needed and improving interoperability with third party PBXs.

Cisco Unified Communications Manager supports early offer (without requiring MTP) when the call gets initiated from one of the following devices:

- SIP phones
- SCCP phones with SCCP v20 support (which provides media port information through the getPort capability)
- MGCP gateways
- Incoming H323 fast start calls
- Incoming early offer SIP trunk calls

Note For the endpoints where the media port information is not available (e.g. H323 slow start calls or delayed offer SIP calls or legacy SCCP phones), Cisco Unified Communications Manager still allocates an MTP in order to provide SDP in the initial INVITE.

Note For calls initiated from any of the previous devices, MTP might be needed due to other reasons such as DTMF/codec mismatch, TRP required on the inbound or outbound trunk, or MTP required on calling side.

For this release, Cisco Unified Communications Manager also enhances interoperability with third party devices during mid-call operations including basic hold/resume operations and during supplementary services, such as transfer and conference. In previous releases, Cisco Unified Communications Manager sent an INVITE with an inactive SDP (a=inactive attribute) to indicate a break in media path, sent a Delayed Offer INVITE to insert music on hold or resume the media stream, and expected a send-recv offer SDP in the 200 OK. Because third party devices often provide an inactive offer SDP in the 200 OK instead of providing a send-recv offer SDP, the media path would remain in an inactive state and cause calls to drop. In this release, Cisco Unified Communications Manager allows you to configure a parameter for an early offer SIP trunk so that Cisco Unified Communications Manager suppresses the sending of inactive or sendonly SDP in mid-call INVITEs. When this parameter gets enabled, Cisco Unified Communications Manager connects the SIP Trunk device directly to the MOH or annunciator device without breaking the existing media stream during call hold or other feature invocation. Similarly, Cisco Unified Communications Manager connects the SIP Trunk device to a line side device directly during call resume without breaking the MOH or annunciator stream. By preventing the far end media stream from getting set to inactive, Cisco Unified Communications Manager should always be able to resume the media path.

Note You should only configure the suppression of inactive or sendonly SDP if you have interoperability issues with third party SIP devices during hold-resume or media resumption for supplementary services. Certain endpoints such as Cisco Unity Connection may not work if you enable this configuration.

In this release, Cisco Unified Communications Manager also provides a send-receive SDP in response to a delayed offer invite in an initial call or mid-call on a SIP trunk if the device connecting to SIP trunk supports GetPort capability. Cisco Unified Communications Manager provides this functionality whether or not the SIP trunk has been configured for early offer. If the device does not support the GetPort capability, Cisco Unified Communications Manager does not insert another MTP to provide a send-receive offer.

Cisco Unified Communications Manager Administration Configuration Tips

To create a trunk that supports early offer, perform the following steps:

Step 1 Create a SIP Profile (**Device > Device Settings > SIP Profile**).

Step 2 Check the **Early Offer Support for voice & video calls (insert MTP if needed)** checkbox.

Note Early Offer configurations on SIP Profile apply to SIP trunk calls. These configurations do not affect SIP line side calls. If this profile is shared between a trunk and a line, only the SIP trunk that uses the profile provides early offer.

Note Because E2E RSVP provides an early offer by including an SDP in the initial INVITE, the early offer and E2E RSVP features are mutually exclusive on the SIP Profile Configuration window. When you choose E2E from the RSVP Over SIP drop-down list box, the Early Offer support for voice and video calls (insert MTP if needed) checkbox gets disabled.

Step 3 Associate the profile that you created with the trunk that you want to support early offer by choosing the profile from the **SIP Profile** drop-down list box on the Trunk Configuration window (**Device > Trunk**), and save and reset the trunk.

Note When checked, the **Media Termination Required** checkbox on the Trunk Configuration window overrides the early offer configuration on the associated SIP Profile. The Cisco Unified Communications Manager sends the MTP IP address and port with a single codec in the SDP in the initial INVITE.

Step 4 If you use SCCP phones with SCCP version 20 support (which provides media port information through the getPort capability), set the following Cisco Unified Communications Manager service parameters (**System > Service Parameters**):

- Get Port Response Timer—Specifies the amount of time in seconds for a SCCP phone with version 20 support making an outgoing call to provide Cisco Unified Communications Manager with port information in order to provide an early offer SDP without using an MTP. The default value equals 2 seconds. The action taken by Cisco Unified Communications Manager if this timer expires before the phone provides port information depends on the setting of the "Fail Call over SIP Trunk if MTP allocation fails" service parameter or the "Fail Call If Trusted Relay Point Allocation Fails" service parameter, depending on the type of device that failed to respond to the port request. The call fails or gets extended as a delayed offer INVITE call on the SIP trunk.
- Fail Call over SIP Trunk if MTP allocation fails—Determines whether Cisco Unified Communications Manager allows a call that requires an MTP to proceed if no MTP resource is available. This parameter also determines the call treatment for an outgoing call over an early offer enabled SIP trunk when the calling device or MTP resource fails to provide a valid audio port during call setup. Choose *False* to allow the call to continue and disable supplementary services, or choose *True* to fail the call if no MTP resources exist or if the audio port of calling device is not available. The default equals *False*.
- Fail Call If Trusted Relay Point Allocation Fails—Determines whether Cisco Unified Communications Manager allows a call that requires a Trusted Relay Point (TRP) to proceed if no TRP resource is available. Choose *False* to allow the call to continue, or choose *True* to fail the call if no TRP resources exist or when the TRP resource fails to provide an audio port for an outgoing call on early offer enabled SIP trunk. Choose the best value for your system based on how you utilize

TRPs. For example, if your system uses TRP for Virtual Routing and Forwarding (VRF) or firewall traversal, set this parameter to True, since Cisco Unified Communications Manager cannot connect audio or video without a TRP resource. If your system uses a TRP for Quality of Service (QoS) enforcement, Cisco Unified Communications Manager can complete the call if a TRP resource is unavailable; however, the call will not have correct Differentiated Service Code Point (DSCP) marking. The default equals *True*.

Note For incoming calls, Cisco Unified Communications Manager times out after 300 milliseconds if the device does not respond to the port request. Cisco Unified Communications Manager provides a sendonly offer SDP with fake port (4000).

To prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services, perform the following steps:

Step 1 Edit the appropriate SIP profile (SIP Profile (**Device > Device Settings > SIP Profile**), and check the **Send send-receive SDP in mid-call INVITE** checkbox.

Step 2 Consider the following interactions:

- When you enable **Send send-receive SDP in mid-call INVITE** for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line. In tandem mode, Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of media path by either sending a delayed offer INVITE or midcall INVITE with send-recv SDP.
- When you enable both **Send send-receive SDP in mid-call INVITE** and **Require SDP Inactive Exchange for Mid-Call Media Change** on the same SIP Profile, the **Send send-receive SDP in mid-call INVITE** overrides the **Require SDP Inactive Exchange for Mid-Call Media Change**, so Cisco Unified Communications Manager does not send an INVITE with a=inactive SDP in mid-call codec updates. For SIP line side calls, the **Require SDP Inactive Exchange for Mid-Call Media Change** checkbox applies when enabled.

Note This checkbox only applies to early offer enabled SIP trunks and has no impact on SIP line calls.

Step 3 To prevent the SDP mode from being set to inactive in a multiple hold scenario, set the **Duplex Streaming Mode** clusterwide service parameter (**System > Service Parameters**) to *True*.

The following limitations and interactions exist for the early offer feature:

- You must use an MTP with IOS version 15.1(2)T or later to support the early offer features.
- SRTP and video—Cisco Unified Communications Manager can advertise secure audio and/or video capabilities in the SDP of and initial INVITE, depending on the capabilities of calling device.
- End-to-end (E2E) RSVP—Because E2E RSVP provides an early offer by including an SDP in the initial INVITE, the early offer and E2E RSVP features are mutually exclusive on the SIP Profile Configuration window. When you choose E2E from the RSVP Over SIP drop-down list box, the Early Offer support for voice and video calls (insert MTP if needed) checkbox gets disabled.

- Single Number Reach (SNR)—When a call gets initiated to trunk single number reach (SNR) destinations from a SIP phone, SCCP v20 phone, or calling device whose media capabilities are available at setup, the INVITE SDP contains the IP address and port of the calling device. When an MTP is required to provide early offer for SNR trunk calls, a separate MTP port gets allocated for each SNR destination.
- IPv6—Cisco Unified Communications Manager sends delayed offer INVITEs for the following IPv6 scenarios, even if you have configured early offer on a SIP trunk:
  - The SIP trunk is configured in IPv6 only mode.
  - The calling device is in IPv6 only mode.
  - The SIP trunk is in dual mode and ANAT is enabled.
  - SIP trunk in dual mode and Media Address Preference is IPv6.
- For the delayed offer SIP call to early offer interworking case, Cisco Unified Communications Manager inserts an MTP to provide SDP on the outgoing call leg. The INVITE contains audio lines only. The INVITE sent on the outgoing leg will have audio media lines only. The calling video capabilities and crypto key of the device are not available to the tandem cluster; thus, no crypto attribute for audio or video media line exists. As a result, the outgoing INVITE SDP contains the IP and audio port of the MTP an no SRTP key or attributes in the asudio media line and no video media lines.
- For the slow start H323 calls to early offer interworking case, Cisco Unified Communications Manager inserts an MTP to provide SDP on the outgoing call leg. The INVITE contains audio lines only. The INVITE sent on the outgoing leg will have audio media lines only. The calling video capabilities and crypto key of the device are not available to the tandem cluster; thus, no crypto attribute for audio or video media line exists. As a result, the outgoing INVITE SDP contains the IP and audio port of the MTP an no SRTP key or attributes in the asudio media line and no video media lines. Cisco Unified Communications Manager escalates to video after receiving video TCS from H323 leg after media cut-through and if call admission control (CAC) allows video and the allocated MTP supports pass-thru and multimedia.
- Cisco Unified Communications Manager sends delayed offer INVITEs for the following scenarios:
  - Mid-call media renegotiation
  - Call hold—Cisco Unified Communications Manager sends a delayed offer INVITE in mid-call when inserting MOH, since the MOH server might not support the same codec as the negotiated audio call. Cisco Unified Communications Manager needs the complete codec list from the far end to renogiatate media.
  - Call resume

Note When a line side device initiates a call transfer and leaves the call, Cisco Unified Communications Manager connects one or two trunk legs and sends a delayed offer INVITE in midcall. Using a delayed offer INVITE ensures that features such as video and SRTP do not get dropped when transfers results in two trunk call legs getting connected.

- Cisco Unified Communications Manager sends a delayed offer INVITE or outgoing call fails when one of the following situations occurs:
  - If an allocated MTP, transcoder or TRP does not support getPort capability and an outbound SIP trunk leg is enabled for early offer, the Cisco Unified Communications Manager does not allocate another media resource for providing early offer.

  - When the "Use Trusted Relay Point" is enabled on SIP trunk (**Device > Trunk**), and the allocated media resource does not support TRP capability or fails to provide the media port, Cisco Unified Communications Manager does not allocate another media resource. This can occur if the MTP or RSVP Agent is not configured for TRP.
  - Depending on the setting of the "Fail Call if MTP allocation fails" or "Fail call if TRP allocation fails" service parameter, Cisco Unified Communications Manager sends a delayed offer or fails the call.
- You need to configure UPDATE and PRACK on the SIP trunk in order to provide ring back in blind transfer cases when the consult call leg on early offer SIP trunk provides inband ringback or announcements. If the trunk is not enabled for PRACK or if the far-end device does not support UPDATE, the transferee does not get a ringback tone.
- As with previous releases, you cannot change the codec order in the offer SDP. Cisco Unified Communications Manager orders the codecs based on an internal list, typically from highest to lowest. To work around this issue, you can create a SIP Normalizaton script to reorder the codecs in the offer SDP.

For assistance in troubleshooting early offer problems, refer to the following table:

Table 1 Troubleshooting Early Offer Problems

Problem	Solution
The initial outgoing INVITE for an early offer SIP trunk call does not contain an SDP.	1. Verify that you check the **Enable Early Offer for voice and video calls** checkbox on the SIP associated with the early offer trunk. 2. Verify that the SIP trunk is not in IPv6 only mode or dual-mode trunk with ANAT or media preference set to IPv6. 3. Verify that calling device is not an IPv6-only device. 4. If initiating calls from pre SCCP v20 device or H323 Slowstart device or delayed offer incoming call, verify that MTP allocation is taking place. 5. Ensure that the caller or SIP trunk media resource group list has an MTP available. Verify that the MTP firmware supports getPort capability. If the MTP image does not support getPort capability, upgrade to newer image, IOS release 15.1(2)T or later. 6. For a SCCP v20 calling device, verify that the device provides the media port in StationPortRes/ DeviceMediaInfoRes. If not, check for a timeout event—GetPortResponseTimer or TimeoutWaitingForPortInfo.

Table 1 Troubleshooting Early Offer Problems

Problem	Solution
An outgoing call for and early offer SIP trunk fails. Cisco Unified Communications Manager does not send an INVITE.	1. If initiating calls from pre-SCCP v20 devices or H323 slowstart or delayed offer incoming trunk, verify that MTP allocation takes place and that the MTP supports SCCP v20. 2. If the MTP allocation fails, do one or more of the following: – Check the configuration for the "Fail Call Over SIP trunk if MTP Allocation Fails" service parameter and set it to FALSE. – Include an MTP in the media resource group list associated with the SIP trunk or default pool. 3. If the MTP image does not support getPort capability, upgrade to newer image, IOS release 15.1(2)T or later. 4. If initiating calls from SCCP v20 devices, check if Cisco Unified Communications Manager times out (typically after 2 seconds) waiting for StationPortRes from the SCCP line device. If yes, the SCCP device needs to be reset or phone logs need to be collected. Also, check the configuration for "Fail Call Over SIP trunk if MTP Allocation Fails" service parameter. If you want Cisco Unified Communications Manager to send a delayed offer invite, set the parameter to *False*.
The outgoing call for early offer SIP trunk always has SDP with one codec and the IP address and port of the MTP.	1. Verify that the "Media Termination Required" is not checked on the Trunk Configuration window for this trunk. 2. If the "Media Termination Required" checkbox is not checked on the Trunk Configuration window for this trunk, check if a media resource is being allocated. Media resources can get allocated for local RSVP, TRP enabled on trunk, early offer, DTMF mismatch, or codec mismatch. 3. Verify that the media resource is configured for pass-through codec.
There is no video during initial call when MTP is inserted in the call.	1. Verify that the "Media Termination Required" is not checked on the Trunk Configuration window for this trunk. 2. Verify that Cisco Unified Communications Manager MTP is not allocated. The Cisco Unified Communications Manager MTP does not support video pass-through. 3. If an IOS MTP is allocated, verify that the IOS MTP is configured with pass-through codec. IOS MTP supports video pass-through. 4. Verify that location call admission control allows video call.

Table 1 Troubleshooting Early Offer Problems

Problem	Solution
Call is not secured when MTP is inserted in the call.	1. Verify that the "Media Termination Required" is not checked on the Trunk Configuration window for this trunk. 2. Verify that the IOS MTP is configured with pass through codec. 3. Verify that call is not initiated from H323 slowstart device or delayed offer trunk.

GUI Changes

The following new checkboxes were added to the SIP Profile Configuration window (**Device > Device Settings > SIP Profile**):

- Early Offer Support for voice & video calls (insert MTP if needed)
- Send send-receive SDP in mid-call INVITE
- Require SDP Inactive Exchange for Mid-Call Media Change

Service Parameter and Enterprise Parameter Changes

The following service parameters were added or changed to support early offer:

- Get Port Response Timer (new)—Specifies the amount of time in seconds for a SCCP phone with version 20 support making an outgoing call to provide Cisco Unified Communications Manager with port information in order to provide an early offer SDP without using an MTP. The default value equals 2 seconds. The action taken by Cisco Unified Communications Manager if this timer expires before the phone provides port information depends on the setting of the "Fail Call over SIP Trunk if MTP allocation fails" service parameter or the "Fail Call If Trusted Relay Point Allocation Fails" service parameter, depending on the type of device that failed to respond to the port request. The call fails or gets extended as a delayed offer INVITE call on the SIP trunk.

Note For incoming calls, Cisco Unified Communications Manager times out after 300 milliseconds if the device does not respond to the port request. Cisco Unified Communications Manager provides a sendonly offer SDP with fake port (4000).

- Fail Call Over SIP Trunk if MTP Allocation Fails (change)—In addition to determining whether an outbound call over a SIP trunk that has the Media Termination Point Required checkbox enabled in Cisco Unified CM Administration will be allowed to proceed if no MTP resource is available, this parameter determines the call treatment for an outgoing call over an early offer enabled SIP trunk when the calling device or MTP resource fails to provide a valid audio port during call setup.
- Fail Call If Trusted Relay Point Allocation Fails (change)—This parameter determines whether a call that requires a Trusted Relay Point (TRP) will be allowed to proceed if no TRP resource is available or also when the TRP resource fails to provide an audio port for an outgoing call on early offer enabled SIP trunk.
- Fail Call If MTP Allocation Fails—This parameter determines whether a call that requires an MTP will be allowed to proceed if no MTP resource is available or also when the MTP resource fails to provide an audio port for a call to an early offer enabled SIP trunk.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

The following traces have been added or changed to support this feature.

The following examples show the changes to the existing SIP trunk trace.

```
001685280 |2010/05/25 13:50:31.980 |100 |AppInfo
|||SIPCdpc(1,100,67,9)||1,100,67,9.1^*^*|//SIP/SIPCdpc(1,67,9)/ci=30801944/ccbId=14961/scb
Id=0/StartTransition: requireInactiveSDPForMidcallMediaChange=0,
isTrunkEnabledForVoiceEO=1
```

Note 1 indicates early offer is enabled for this call; 0 indicates that early offer is disabled.

```
001685289 |2010/05/25 13:50:32.001 |100 |SdlSig |PolicyAndRSVPRegisterReq |wait
|RSVPSessionMgr(1,100,91,1) |SIPCdpc(1,100,67,9)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801944 Branch= 0 reg=Default cap=0 loc=0 MRGLPkid=1db1ba42-9575-e3dc-ba78-fb11d56db546
PrecLev=5 VCall=F VCapa=F VCapCount=0 regiState=0 medReq=0 dataCapFl=2 IsEmccD=F
EmccDName=to-ccm84 rcId= ipMode=0 eoType=2 getPort=F sRTP=F cryptocap=0 tm=16
DTMF(wantRecep=1 provOOB=1 suppMeth=1 Cfg=1 PT=0 reqMed=0) hInCodec=F distMed=F mediaEP=F
rsvpQoSType=0 qosFallback=F status=0 sipOfferNeededInd=T hasSDP=F geolocInfo={geolocPkid=,
filterPkid=, geolocVal=, devType=8}
```

Note The values for eoType include: None(0), early offer for G.Clear (1), early offer for voice and video (2), and early offer for G.Clear voice and video (3).

```
001685353 |2010/05/25 13:50:32.087 |100 |SdlSig |PolicyAndRSVPRegisterRes
|outCall_waitRSVPRes |SIPCdpc(1,100,67,9) |RSVPSession(1,100,93,5)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801944 Branch= 0 Status=1 rsvpPol=1 vCall=F e2eRSVPInserted=F eoStatus=1 hasSDPMsg=T
RSVPAgent: confID =0 ci =0 capCt =0 reg= mtpType =2 agentCt =0 agentAllo =0 RemoAgent=F
DevCap=0 ipAddrMode=0
```

Note The valid values for eoStatus include: None(0), early offer for voice and video (1), early offer for G.Clear (2), Continue delayed offer (3), and failed call (4).

The following examples show the new traces added for StationD (SCCP device) participating in an early offer call:

```
001685325 |2010/05/25 13:50:32.064 |100 |SdlSig |DeviceMediaInfoReq |restart0
|StationD(1,100,50,13) |RSVPSession(1,100,93,5)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801943 confID=30801943 callRefID=30801943 counter=1 mediaType=1 iptype=0 PPID=16777217
reqCode=1
001685327 |2010/05/25 13:50:32.064 |100 |SdlSig |StationPortReq |restart0
|StationD(1,100,50,13) |StationCdpc(1,100,51,1)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0]
confID=30801943 PPID=16777217 CI=30801943 transportType=1 addrType=0 mediaType=1 .
```

Response from the SCCPv20 device

```
001685328 |2010/05/25 13:50:32.081 |100 |AppInfo
|||StationInit(1,100,49,1)||1,100,49,1.100207^172.18.199.61^SEP001319ACCA00|StationInit:
(0000013) PortRes IpAddr=0x399eb00, Port=31780, RTCPPort=0, confID=30801943, PPID=16777217
```

```
001685330 |2010/05/25 13:50:32.081 |100 |SdlSig |StationPortRes |outgoing_call_proceeding3
|StationCdpc(1,100,51,1) |StationD(1,100,50,13)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0]
CI=30801943 confID=30801943 ptpID=16777217 ipaddr=0x{ac,12,c7,3d,0,0,0,0,0,0,0,0,0,0,0,0}
port=31780 =.type=0 . RTCPPort=0 mediaType=1

001685331 |2010/05/25 13:50:32.082 |100 |SdlSig |DeviceMediaInfoRes |wait
|RSVPSessionMgr(1,100,91,1) |StationCdpc(1,100,51,1)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801943 confID=30801943 callRefID=30801943 mediaType=1 iptype=0 PPID=16777217 reqCode=1
port=31780 RTCPPort=0 ipAddrType=0 ipv4=172.18.199.61 status=0
```

The following example shows new traces for media layer for early offer call when MTP allocation is required

```
001686458 |2010/05/25 13:50:48.535 |100 |SdlSig |AuEarlyOfferConnectReq |waitForAll
|MediaCoordinator(1,100,125,1) |RSVPSession(1,100,93,6)
|1,100,49,1.100222^172.18.201.82^SEP0014F2E982F1 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] Party1:
CI=30801945 capCount=7 region=Default xferMode=4 mrid=0 audioId=0 videoCap=F dataCap=2
activeCap=0 cryptoCapCount=0 flushIns=0 dtmCall=0 dtmPrimaryCI=0 IFPid=(0,0,0,0) dtMedia=F
honorcodec=F EOType=0 MohType=0 Party2: CI=30801946 capCount=0 region=Default xferMode=16
mrid=0 audioId=0 videoCap=F dataCap=2 activeCap=0 cryptoCapCount=0 flushIns=0 dtmCall=0
dtmPrimaryCI=0 IFPid=(0,0,0,0) dtMedia=F honorcodec=F EOType=2 MohType=0 videoCall=F
confID =0 ci =0 capCt =0 reg= mtpType =2 agentCt =0 agentAllo =0 RemoAgent=F DevCap=0
ipAddrMode=0 mtpInsReason=32 hasSDP=F
```

Note Valid values for mtpInsReasons include: None (0), TRP Side B (1), TRP Side A (2), Transcoder Side A (4), MTP Side A (8), DTMF mismatch (16), early offer (32).

```
001686676 |2010/05/25 13:50:48.646 |100 |SdlSig |AuEarlyOfferConnectReply |wait
|RSVPSession(1,100,93,6) |MediaCoordinator(1,100,125,1)
|1,100,49,1.100223^172.18.197.154^MTP_sinise |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0]
ciParty1=30801945 ciParty2=30801946 devicePidParty1=(1,100,50,3)
devicePidParty2=(1,100,67,10) err=0 videoFlag=F hasSDP=T.
```

Note Valid values for Err codes for media resource allocation failures include: No Error (0), TRP allocation Side B (1), TRP Side A (2), Transcoder Side A (3), MTP Side A (4), MTP for DTMF mismatch (5), MTP for early offer (6).

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

EMCC Device Maintains Network Setting

When a user uses a phone in a visiting cluster to log into the user Extension Mobility profile, the phone inherits the default provisioning, network, and security settings (specifically, the configuration in the Product Specific Configuration Layout section of the Phone Configuration window) from the home cluster. This behavior may override local security and network settings that are in place in the visiting cluster. Some of the parameters have firmware defaults that the system administrator cannot change until a fix is provided.

Interoperability with Cisco Unified Customer Voice Portal Release 7.0(2)

Cisco Unified Communications Manager Release 7.1(5) and later is compatible with Cisco Unified Customer Voice Portal Release 7.0(2).

IP Phone Service Enhancements

There are two new IP Phone service categories available for Android in Cisco Unified Communications Manager 8.5(1):

- Web Link—This is a service category that you can add by specifying its URL in the IP Phone Services Configuration window. When provisioned, the service displays in the application menu of the device. When the user invokes the URL, it opens in the browser.
- Web Widget—This service category is a standalone W3C web widget application that can be installed separately.

Mobility Feature Enhancements

Updates to the "Cisco Unified Mobility" Chapter

The following topics in the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* were updated with new information:

- Methods for Enabling and Disabling Mobile Connect
- Mobility Enterprise Feature Configuration
- Handoff Mobility Configuration
- Mobility Profile Configuration

Updates to the "Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator" Chapter

The following topic was added to the "Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration" chapter of the *Cisco Unified Communications Manager Features and Services Guide* with detailed information about the new feature:

- **Session Resumption**—This feature provides one-touch reconnect to the last dialed target in case of any unexpected DVO-F call drop. This feature helps users who are making DVO-F calls and who experience a network failure. Prior to the implementation of this feature, if the mobile user pressed Redial, the redial number specified the feature access DN, which is an internally configured DID number, not a dialable number. Cisco Unified Communications Manager treated the call as an Enterprise Feature Access call, and the user could not connect to the last redial target. With the implementation of this feature, when the user presses Redial, Cisco Unified Communications Manager reconnects the mobile user with the actual target DN.

The Session Resumption feature is implemented for the following reason:

– Mobile call failure is very common in the cellular network. For DVO-F calls, the dialed number that is stored on the mobile handset specifies the DVO-F service access number, which is an internally configured DID number. When the user presses **Redial** on the user handset, the stored number has already been dialed, so Cisco Unified Communications Manager cannot reach the original target.

Upon implementation of the Session Resumption feature, Cisco Unified Communications Manager stores the target number DN when the DVO-F call initially gets made. If the user presses **Redial** after a network failure, Cisco Unified Communications Manager receives the service access number, which Unified CM replaces with the stored target DN. Thus, the redial request succeeds: either a new call gets extended to the original target, or the original call gets reconnected, depending on whether the original call got released.

Configuration Details

The following configuration details apply to the Session Resumption feature.

– The Session Resumption feature uses the setting of the Redial Await Timer service parameter, which you configure in the Service Parameter Configuration window (**System > Service Parameters**) for the Cisco CallManager service in the Clusterwide Parameters (System - Mobility) pane. The Redial Await Timer service parameter has a default setting of 180 seconds (3 minutes), but can be set to any value between 0 seconds and 300 seconds (5 minutes). Setting the Redial Await Timer service parameter to 0 seconds disables the timer and the Session Resumption feature.

– After the Redial Await Timer expires in the case of a DVO-F call that was interrupted due to network failure, the record of the original target DN for this DVO-F call gets deleted. Any Redial call that is placed after the timer expires gets invoked as an enterprise feature access (EFA) call: the Session Resumption feature does not get triggered.

– Upon network failure, the Session Resumption feature succeeds if the DVO-F call is in either the alerting or the connected state.

– If a Redial call gets extended to a busy target DN, the user receives a busy tone.

New "Cisco Mobile VoiP Clients" Chapter

The new "Cisco Mobile VoiP Clients" chapter of the *Cisco Unified Communications Manager Features and Services Guide* contains information and details about these new features:

- **Dial-via-Office (DVO) Optimization Settings for Toll Reduction**—This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. This feature benefits the mobile user by allowing the user to find the least cost when making a mobile call. The DNIS pool provides a list of Direct Inward Dialing (DID) numbers so that the user, if roaming, can choose a non-international number for the mobile call. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.

  This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. This feature benefits the mobile user by allowing the user to find the least cost when making a mobile call. The DNIS pool provides a list of Direct Inward Dialing (DID) numbers so that the user, if roaming, can choose a non-international number for the mobile call. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.

  Reasons for DVO Optimization Settings for Toll Reduction

The following reasons make this feature desirable:

- Administrator can decide upon the DVO call type, DVO-F or DVO-R, for least cost call routing. In certain regions and with certain service providers, DVO-F can be more economical for mobile users; in other regions, DVO-R can be more economical. For example, in regions where incoming calls are free for mobile phone users, configuring a DVO-R call for mobile phone users achieves least cost call routing.
- Scalability—Multiple users in a given region can use a single mobility profile, which comprises region, service provider, location, and so forth. Here, "users" refers to the clients under actual end users. The administrator does not need to create a mobility profile for each end user.
- Single DID within a cluster for all DVO-F calls—For such DVO-F calls, the client makes an incoming call to Cisco Unified Communications Manager by using a particular DID.
- Multisite cluster—For a multisite cluster, a client in cluster A (such as the UK) uses the DID of cluster B (such as San Jose) for DVO-F calls, which incurs costs.
- DVO-R—Trunk allows calls that originate from a local DID. At times, when a client makes an outgoing DVO-R call, the client trunk may not allow an outgoing call if the caller ID does not lie in a specific range. For example, if a UK client invokes DVO-R, the callback call from the trunk at the San Jose cluster shows 408. When this call reaches the UK, the service provider trunk may not recognize the 408 and therefore not allow the call. Therefore, the caller IDs need to specify the local identifiable values.

Characteristics of DVO Optimization Settings for Toll Reduction

This feature involves the use of mobility profiles, which the administrator configures by using the **Call Routing > Mobility > Mobility Profile** menu path in Cisco Unified Communications Manager Administration.

DVO Optimization Settings for Toll Reduction do not change the alternate callback mechanism that DVO-R calls use: the client continues to control alternate callback.

- **Enable/Disable Mobile Connect From Mobile Phone**—This feature allows the Cisco Unified Mobile Communicator client to change the Mobile Connect status dynamically and keep the Mobile Connect Status between Cisco Unified Communications Manager and the client in sync. This feature provides the flexibility to the end user: the end user can change the user Mobile Connect status from the user mobile phone, not just from the GUI website.

  Prior to Release 8.5(1) of Cisco Unified Communications Manager, Cisco Unified Communications Manager sent Mobile Connect status updates to the Cisco Unified Mobile Communicator client via Cisco Unified Mobility Advantage by AXL messages. Direct SIP messages between the Cisco Unified Mobile Communicator client and Cisco Unified Communications Manager now allow the client to change the client Mobile Connect status.

  Beginning with Release 8.5(1) of Cisco Unified Communications Manager, the Cisco Unified Mobile Communicator client can update its Mobile Connect status directly. The following processing takes place:

  - When the Cisco Unified Mobile Communicator registers with Cisco Unified Communications Manager for the first time, Cisco Unified Communications Manager sends a 200 OK Response message, then sends an out-of-dialog REFER message to Cisco Unified Mobile Communicator with the current Cisco Unified Mobile Communicator Mobile Connect status. This sequence takes place only for the first registration, not for any refresh registrations.
  - Whenever the Mobile Connect status changes by means of any Cisco Unified Communications Manager interface, Cisco Unified Communications Manager immediately sends an out-of-dialog REFER message to the Cisco Unified Mobile Communicator client with the updated Mobile Connect status. The client can thus update the mobile phone display with the correct Mobile Connect status.

  - If the Cisco Unified Mobile Communicator client changes the Mobile Connect status, the following processing takes place:

    The Cisco Unified Mobile Communicator client sends an out-of-dialog REFER message to Cisco Unified Communications Manager with the changed Mobile Connect status.

    Cisco Unified Communications Manager stores the changed Mobile Connect status in the database and notifies the other interested Cisco Unified Communications Manager components.

    Cisco Unified Communications Manager also sends another out-of-dialog REFER message to the Cisco Unified Mobile Communicator client with the changed Mobile Connect status so that the client knows that the status has been updated.

- **Direct Connection From Cisco Unified Communications Manager to Mobile Client Without Proxy Server**—This feature provides server-side support for Cisco Unified Mobile Communicator clients to connect to Cisco Unified Communications Manager directly and thus eliminate Cisco Unified Mobility Advantage in the deployment. In previous releases, Cisco Unified Communications Manager connections to Cisco Unified Mobile Communicator required the services of a Cisco Unified Mobility Advantage server. This feature thereby reduces the necessary configuration and requires less equipment. Cisco Unified Communications Manager adjusts to support direct connection with the Cisco Unified Mobile Communicator.

  Beginning in Release 8.5(1) of Cisco Unified Communications Manager, Cisco Unified Mobile Communicator registers directly with Cisco Unified Communications Manager and no longer needs to register with the Cisco Unified Mobility Advantage server.

  Registration between the Cisco Unified Mobile Communicator client and Cisco Unified Communications Manager takes place over a separate TCP port. (The shared or pooled connection that was used by the Cisco Unified Mobility Advantage server is not used.) Keepalive messages between Cisco Unified Mobile Communicator and Cisco Unified Communications Manager remain the same as those passed between Cisco Unified Communications Manager and Cisco Unified Mobility Advantage. That is, keepalive messages occur with a 120 second refresh time. Cisco Unified Mobile Communicator registration with Cisco Unified Communications Manager introduces no new alarms, and registration takes place over the SIP channel without OWLP involvement.

  If the client is running on the iPhone and Cisco Unified Mobile Communicator is unable to complete the SIP dialog, the Cisco Unified Communications Manager retains the PSTN call. (The PSTN call does not drop even if the SIP stat times out.) For example, if Cisco Unified Communications Manager does not receive an ACK message after it sends a 200 OK message, the PSTN call gets retained.

Cisco Unified Communications Manager Administration Configuration Tips

In Cisco Unified Communications Manager Administration, use the **Call Routing > Mobility > Mobility Profile** menu path to configure mobility profiles, which are new in Release 8.5(1) of Cisco Unified Communications Manager Administration.

Mobility profiles specify profiles where you can configure Dial-via-Office Forward or Dial-via-Office Reverse settings for a mobile client. After you configure a mobility profile, you can assign it to a user or to a group of users, such as the users in a region or location. You specify either DVO-F or DVO-R for a particular mobility profile, but you configure both the DVO-F and DVO-R settings for the mobility profile.

Mobility profiles can associate with standalone Cisco Unified Mobile Communicator mobile identity or with Cisco Unified Mobile Communicator-enabled dual-mode mobile identity. Standard, single-mode remote destinations cannot associate with a mobility profile.

Mobility profile settings can be changed only by administrators: users cannot change the settings in a mobility profile. Also, users do not need to adjust any settings to a mobility profile by logging into their Cisco Unified CM User Options pages.

Note If no mobility profile exists for a client and the client opts to let the server choose, the default DVO call type specifies Dial-via-Office Reverse (DVO-R).

Consider the following design issues before you start to configure mobility profiles:

- If a client associates with a mobility profile and a DVO-R call is configured, the caller ID value in the 183 SIP message gets retrieved according to the following preference order:
  1. DVO-R caller ID from the mobility profile (if this value is configured in the mobility profile)
  2. EFA DN from mobility profile (if this value is configured in the mobility profile)
  3. Default EFA DN

Note The administrator must configure the caller ID value in at least one of the preceding settings for the DVO-R call to succeed.

- If a client associates with a mobility profile and a DVO-F call is configured, the DID value in the 183 SIP message gets retrieved according to the following preference order:
  1. DVO-F service access number from mobility profile (if this value is configured in the mobility profile)
  2. DVO-F EFA DN from mobility profile (if this value is configured in the mobility profile)
  3. Default service access number, which is configured in the Service Parameter Configuration window
  4. Default EFA DN

Note For a DVO-F call, the client needs to make an incoming call to Cisco Unified Communications Manager that terminates at a particular DID. The administrator must configure this DID in at least one of the preceding settings for the DVO-F call to succeed.

Cisco Unified Communications Manager identifies an incoming PSTN call (made by the client) as DVO-F by matching the called number (that is, the DID number that was sent in the 183 SIP message) in the following priority order:

- If a mobility profile associates with the client
  1. DVO-F EFT DN from mobility profile (if this value is configured)
  2. DVO-F service access number from mobility profile (if this value is configured)
- If no mobility profile associates with the client:
  1. Default EFA DN
  2. Default service access number

Also consider the following requirements when you configure mobility profiles:

- Administrator should configure the PSTN gateway so that matching of the called party can take place.

- EFA DN and service access number always comprise a pair: both of these values get retrieved from the mobility profile and must match in the mobility profile, or both default values get retrieved and the default values must match.

GUI Changes

The **Call Routing > Mobility Configuration** menu option was replaced by the following menu options:

- **Call Routing > Mobility > Enterprise Feature Access Configuration**—This menu option brings up the Mobility Enterprise Feature Configuration window, which comprises the following settings:

  Access Number Information

  - Number
  - Route Partition
  - Description
  - Default Enterprise Feature Access Number

- **Call Routing > Mobility > Handoff Configuration**—This menu option brings up the Handoff Mobility Configuration window, which comprises the following settings:

  Handoff Configuration Information

  - Handoff Number
  - Route Partition

  Note No Find/List window exists for this menu option, because only one handoff number can be configured for a Cisco Unified Communications Manager system.

- **Call Routing > Mobility > Mobility Profile**—This menu option brings up the Mobility Profile Configuration window, which comprises the following settings:

  Mobility Profile Information

  - Name
  - Description
  - Mobile Client Calling Option

  Dial-via-Office Forward Configuration

  - Service Access Number
  - Enterprise Feature Access Number/Partition

  Dial-via-Office Reverse Callback Configuration

  - Callback Caller ID

The Remote Destination Configuration window added the following setting:

- Mobility Profile

Service Parameter and Enterprise Parameter Changes

The Redial Await Timer service parameter, new in Release 8.5(1) of Cisco Unified Communications Manager Administration, is used to configure the Dial-via-Office Redial feature. See the description of the Dial-via-Office Redial feature for details.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Platform

The Cisco UCS C200 High-Density Rack-Mount Server and the Cisco UCS C210 General-Purpose Rack-Mount Server are only supported through VMware ESXi. Hardware-specific components such as BIOS and RAID controller firmware flashing and configuration, hardware SNMP, and Cisco Integrated Management Controller (CIMC) must be managed manually and are independent of the CUCM applications installed on these servers. The VMware vCenter product can be used for virtual machine management and host configuration. The Cisco UCS C200 and C210 servers are different from the Cisco 7800 Series Media Convergence Servers, which run an appliance operating system natively and automatically manage hardware components.

For more information, refer to the Unified Communications Virtualization wiki at http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization.

Q.SIG Tunneling over SIP

Description

Cisco Unified Communications Manager supports QSIG tunneling over a SIP trunk. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement.

Cisco Unified Communications Manager Administration Configuration Tips

For Cisco Unified Communications Manager to support QSIG tunneling over a SIP trunk, you must choose the QSIG option in the Tunneled Protocol drop-down list box and check the Path Replacement Support check box in the Trunk Configuration window in Cisco Unified Communications Manager Administration. By default, Cisco Unified Communications Manager sets the option in the Tunneled

Protocol drop-down list box to None; after you configure the QSIG Tunneled Protocol option, the Path Replacement Support check box automatically becomes checked. If you do not require path replacement over Annex M.1 or QSIG-tunneled trunks, you can uncheck the check box.

Note Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.

To turn off RPID headers on the SIP gateway, apply a SIP profile to the voIP dial peer on the gateway, as shown in the following example:

```
voice class sip-profiles 1000
request ANY sip-header Remote-Party_ID remove
response ANY sip-header Remote-Party-ID remove

dial-peer voice 124 voip
destination-pattern 3...
signaling forward unconditional
session protocol sipv2
session target ipv4:<ip address>
voice-class sip profiles 1000
```

GUI Changes

The Device menu in Cisco Unified Communications Manager Administration supports the following new fields and check boxes for a SIP trunk type:

- Tunneled Protocol
- QSIG Variant
- ASN.1 ROSE OID Encoding
- Path Replacement Support check box
- Transmit UTF-8 Names in QSIG APDU check box

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

You can export the configuration details for the following QSIG fields by using the Export Data page in BAT:

- Tunneled Protocol with option for SIP Trunk
- QSIG Variant for SIP Trunk
- Path Replacement Support for SIP Trunk
- Name APDU UTF-8 Encoding for SIP Trunk

To access the Export Data page, navigate to **Bulk Administration > Import/Export > Export**.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

SIP Trunk Security Enhancements

Description

This enhancement provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, irrespective of the signaling transport.

Depending upon the user configuration selection, negotiated media and negotiated transport values, Cisco Unified Communications Manager will decide the security status of the call leg. If the administrator enables the sRTP Allowed check box and selects the When using sRTP and TLS option, Cisco Unified Communications Manager reports encrypted security status when sRTP and TLS are negotiated media and negotiated transport values, respectively. If the administrator enables the sRTP Allowed check box and selects the When using sRTP only, Cisco Unified Communications Manager reports encrypted security status only when sRTP media is negotiated, regardless of what transport the call is using. Apart from this, Cisco Unified Communications Manager call control also considers incoming Call-Info header security status to determine the overall security level of the call.

Cisco Unified Communications Manager Administration Configuration Tips

On the SIP Trunk Configuration window, a new drop-down list box, Consider Traffic on this Trunk Secure, below the sRTP Allowed check box, consists of the following two selections:

- When using both sRTP and TLS
- When using only sRTP

The Consider Traffic on this Trunk Secure field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport.

GUI Changes

A new field exists on the SIP Trunk Configuration window with two options.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

See the *Cisco Unified Communications Manager Security Guide* for more information.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Single Sign On

Description

The single sign on feature allows end users to log into Windows, then use the following Cisco Unified Communications Manager applications without signing on again:

- User Options Pages
- Cisco Unified Communication interface for Microsoft Office Communicator

Cisco Unified Communications Manager Administration Configuration Tips

The following single sign on system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager release 8.5(1) on each server in the cluster

The feature requires the following third-party applications:

- Microsoft Windows Server 2003 or Microsoft Windows Server 2008
- Microsoft Active Directory
- ForgeRock Open Access Manager (OpenAM) version 9.0

The single sign on feature uses Active Directory and OpenAM in combination to provide single sign on access to client applications.

These third party products must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible on the network to all client systems and the Active Directory server.
- The Active Directory (Domain Controller) server, Windows clients, Cisco Unified Communications Manager, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- No third-party products may be installed on the Cisco Unified Communications Manager server.

- The clocks of all the entities participating in SSO must be synchronized

See the third-party product documentation for more information about those products.

Configuring OpenAM

Perform the following tasks using OpenAM:

- Configure policies in OpenAM for the following:
  - CUCM User and UDS web application
  - Query Parameters
- Configure a J2EE Agent Profile for Policy Agent 3.0.
- Configure a Windows Desktop SSO login module instance.
- Configure “Login Form URI” and “OpenAM Login URL” for the PA.
- Disable local user profiles.

Importing the OpenAM Certificate into Cisco Unified Communications Manager

Because communication between Cisco Unified Communications Manager and OpenAM is secure, you must obtain the OpenAM security certificate and import it into the Cisco Unified Communications Manager tomcat-trust store. Configure the OpenAM certificate to be valid for 5 years.

For information about importing certificates, see the *Cisco Unified Communications Operating System Administration Guide*.

Configuring Windows Single Sign On with Active Directory and OpenAM

This section describes how to configure Windows single sign on with Active Directory and OpenAM. This procedure allows Cisco Unified Communications Manager to authenticate with Active Directory.

Procedure

Step 1 In Active Directory, create a new user with the OpenAM Enterprise host name (without the domain name) as the User ID (login name).

Step 2 Create keytab files on the Active Directory server.

Step 3 Export the keytab files to the OpenAM system.

Step 4 In OpenAM, create a new authentication module instance with the following configuration:

- The type is Windows Desktop SSO.
- The realm attributes are determined as follows:
  - Service Principal: Enter the principal name that you used to create the keytab file.
  - Keytab File Name: Enter the path where you imported the keytab file.
  - Kerberos Realm: Enter the domain name.
  - Kerberos Server Name: Enter the FQDN of the Active Directory server.
  - Authentication level: Enter **22**.

Configuring Internet Explorer for Single Sign On

The single sign on feature supports Windows clients running Internet Explorer version 6.0 and higher. Do the following tasks to configure Internet Explorer to use single sign on:

- Select the Integrated Windows Authentication option.
- Create a custom security level configured as follows:
  - Select the Automatic Logon Only in Intranet Zone option
  - Select all of the options for sites.
  - Add OpenAM to the local zone, if it not already added.
- Do the following tasks for Internet Explorer 8.0 running on Windows 7:
  - Disable Protected Mode.
  - Under registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\, add DWORD value SuppressExtendedProtection - 0x02.

Configuring FireFox for Single Sign On

The single sign on feature supports Windows clients running FireFox version 3.0 and higher.

To configure Firefox to use single sign on, enter the trusted domains and URLs that are permitted to engage in SPNEGO Authentication with the browser into the network.negotiate-auth.trusted-uris preference.

Running CLI Commands for Single Sign On

The following sections describe the CLI commands that configure single sign on.

utils sso enable

This command enables and configures single sign on.

Command Syntax

utils sso enable

Usage Guidelines

This command starts a single sign on configuration wizard. You get prompted for the information described in Table 2. Answer each prompt, then press **Enter** to continue.

Caution Enabling single sign on restarts the Cisco Unified Communications Manager web server (Tomcat).

You must run this command on all nodes in a cluster.

Table 2 Single Sign On Configuration Wizard Prompts

Information That the Prompt Requests	Description
URL of the Open Access Manager (OpenAM) server	The URL that you configured for the OpenAM server.
Relative path where the policy agent should be deployed	Enter the path on the Cisco Unified Communications Manager where the policy agent will get deployed. This path is relative to the “agentapp” directory. This path must match the path that you configured for the J2EE Agent Profile for Policy Agent 3.0.

Table 2 Single Sign On Configuration Wizard Prompts (continued)

Information That the Prompt Requests	Description
Name of the profile configured for this policy agent	The name of the profile that you created for this policy agent in OpenAM.
Password of the profile.	—
Login module instance name configured for Windows Desktop SSO	The name of the login module instance for Windows Desktop SSO that you configured in OpenAM.

Example

```
admin:utils sso enable
         ***** W A R N I N G *****
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): yes
Enter URL of the Open Access Manager (OpenAM) server:
https://ssoserver.cisco.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: CUCMUser
Enter the password of the profile name: ********
Enter the login module instance name configured for Windows Desktop SSO: CUCMUser
Validating connectivity and profile with AM Server:
https://ssoserver.cisco.com:8443/opensso
Valid profile
Enabling SSO ... This will take upto 5 minutes
SSO Enable Success

Please make sure to execute this command on all the nodes in the cluster.
```

utils sso disable

This command disables single sign on.

Command Syntax

utils sso disable

Usage Guidelines

Caution Disabling single sign on restarts the Cisco Unified Communications Manager web server (Tomcat).

You must run this command on all nodes in a cluster.

utils sso status

This command displays the status and configuration parameters of single sign on.

Command Syntax

utils sso status

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

The following existing alarms are modified for Single Sign On and SmartCard Authentication:

- authFail
- authSuccess
- authLdapInactive

The following new alarms are generated for Single Sign On and SmartCard Authentication:

- LDAPServerUnreachable
- SSODisabled
- SSONullTicket
- SSOServerUnreachable
- SSOUserNotInDB

For more information on alarm definitions, refer Serviceability - Alarms for Single Sign On and SmartCard Authentication, page 81.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

SIP Header Enhancements for Call Recording

Description

Release 8.5(1) of Cisco Unified Communications Manager introduces enhancements to the SIP headers that are used in the SIP messages that are sent to the recorder when call recording calls are made. These enhancements entail the following changes:

- Cisco Unified Communications Manager sends both the agent (near-end) and customer (far-end) call information to the recorder via SIP messages. Messages travel through the SIP trunk. (Prior to this enhancement, only the near-end information was sent via SIP messages and the far-end information required a CTI connection to Cisco Unified Communications Manager.)
- The enhancement increases scalability: the recorder no longer requires a CTI connection to Cisco Unified Communications Manager to obtain far-end call information from Cisco Unified Communications Manager.
- The enhancement supports automatic recording through use of the Open Recording Architecture (ORA) Cisco Zephyr recorder. Thus, a complete call-recording solution that uses only Cisco products is now available. The Cisco Zephyr recorder provides a basic and powerful recording capability and does not rely on CTI to obtain the far-end information.

Previously, Cisco Unified Communications Manager only sent a SIP INVITE message to a recorder. The From header contains the near-end call info. The near-end call information contains refci or the call ID of the near-end party, near-end device name, near-end directory number or address.

With the SIP header enhancement, the far-end call information gets added to the INVITE message From header. The far-end call information contains farendRefCI or the call ID of the far-end party, far-end device name, and far-end directory number.

Whenever the far-end call info changes due to feature interaction, Cisco Unified Communications Manager sends a SIP UPDATE message to the recorder.

The From header also includes an *isfocus* indicator, which indicates that an agent is in a conference call.

Examples of the previous INVITE message and the new INVITE and UPDATE messages follow.

Previous From Header in SIP INVITE Message

```
From: <sip:3005@10.89.81.56;x-nearend;x-refci=25471846;x-nearenddevice=SEP001B535CDC62 >;
```

New From Header in SIP INVITE and UPDATE Messages

```
From:
<sip:3005@10.89.81.56;x-nearend;x-refci=25471846;x-nearenddevice=SEP001B535CDC62;x-farendr
efci=25471847;x-farenddevice=CFB_2;x-farendaddr=b097865452:isfocus>;
```

In the new From header, the **text in bold** indicates the new information that the SIP header enhancement includes.

Call flow diagrams and detailed explanations of the following use cases were added to the "Monitoring and Recording" chapter of the *Cisco Unified Communications Manager Features and Services Guide*. Each use case explains how the SIP header information is enhanced for calls that involve an agent that is configured for automatic call recording.

- Automatic Call Recording
- Local Cluster Far-End Party Hold/Resume
- Far-End Party Transfers Call to Another Far-End Party in Local Cluster
- Near-End Party Transfers Call to Another Near-End Party in Local Cluster
- Far-End Party Transfers Call to CFNA-Enabled Party

- Far-End Party in Local Cluster Creates Conference
- Near-End Party in Local Cluster Creates Conference
- Far-End Party in Remote Cluster Transfers Call to Another Party in Remote Cluster
- Far-End Party in Remote Cluster Blind-Transfers Call to Remote-Cluster Party That Has CFNA Configured
- Far-End Party in Remote PBX Transfers Call to Phone in Local Cluster
- Remote PBX Far-End Party Transfers Call to Local Phone With Path Replacement
- Far-End Party Transfers Call Across DMS Gateway
- Desktop Pickup of Mobile Phone Call
- Far-End Party Sends Call to Mobile Phone for Mobile Phone Pickup
- Far-End Party in Remote Cluster Creates Conference

Cisco Unified Communications Manager Administration Configuration Tips

To provide Cisco Unified Communications Manager with additional information when the far-end party in a remote cluster creates a conference, configure the Deliver Conference Bridge Identifier check box in the SIP Profile Configuration window. Follow these guidelines:

- To allow the conference bridge identifier (the b-number of the conference bridge) to pass from cluster Cisco Unified CM2 to cluster Cisco Unified CM1, the administrator creates a SIP profile in cluster Cisco Unified CM2, checks the Deliver Conference Bridge Identifier check box, and assigns the SIP profile to SIPTrunkToCluster1 in cluster Cisco Unified CM2. The administrator also creates a SIP profile in cluster Cisco Unified CM1 and assigns this SIP profile to the SIPTrunkToCluster2 in cluster Cisco Unified CM1.

The following topic was added to the "Monitoring and Recording" chapter of the *Cisco Unified Communications Manager Features and Services Guide* to supplement the procedures for setting up call recording:

- Create SIP Profile for Recording

The SIP header enhancements for Call Recording present the following limitations:

- Recording and Call Hold and Resume—Cisco Unified Communications Manager does not update the recorder when the far-end party puts the call on hold. The recorder will be updated only when a different far-end party resumes the call.

  Cisco Unified Communications Manager updates a recorder when the far-end call information changes. The far-end call information contains a call ID, directory number, and device name. If one of these parameters changes, the far-end call information changes.

  If a far-end party holds and resumes a call from the same device, Cisco Unified Communications Manager does not update a recorder.

- Recording and Call Park and Retrieve—If the far-end party in a remote cluster parks the call, Cisco Unified Communications Manager updates the recorder with an empty far-end party address, provided the remote cluster connects to the local cluster via a SIP trunk or an H323 intercluster trunk. Cisco Unified Communications Manager updates the recorder again when the far-end party retrieves the call either from the same or a difference device. Cisco Unified Communications Manager does not update the recorder if the far-end party that parks the call is in the local cluster. In this case, Cisco Unified Communications Manager only updates the recorder when the call gets retrieved from a different device.

For remote Call Park and Retrieve, the remote Cisco Unified Communications Manager sends the display name Call Park update. This update contains an empty directory number/address; therefore, the far-end address changes to empty. Due to the far-end address change, the local Cisco Unified Communications Manager sends the update with the empty far-end address to the recorder.

- Recording and Call Forward No Answer (CFNA)—If the far-end party in a remote cluster blind-transfers the call to a party that has CFNA enabled, Cisco Unified Communications Manager updates the recorder with the ringing party as the far-end party address, provided the remote cluster connects to the local cluster with a SIP trunk or an H.323 intercluster trunk. Cisco Unified Communications Manager updates the recorder again when the call gets forwarded to the CFNA target. Cisco Unified Communications Manager does not update the recorder if the far-end party that blind-transfers g the call is in the local cluster. In this case, Cisco Unified Communications Manager only updates the recorder when the CFNA target answers the call.

  When a remote call becomes active, the call state stays active in a local cluster. When a remote far-end party performs a blind call transfer to a new remote far-end party and the party rings, the local Cisco Unified Communications Manager still sees the call state as active. Thus, for remote Call Forward No Answer, the local Cisco Unified Communications Manager sends UPDATE messages to the recorder for a new party because the call state is active.

  When a local call becomes active, the call state can change from active to ringing state. The local Cisco Unified Communications Manager can find out a current call state. Thus, for local Call Forward No Answer, the local Cisco Unified Communications Manager sends UPDATE messages to the recorder after a new far-end party answers a call.

- Recording and Conference Chaining—If two or more near-end parties are in two or more conferences that are chained together, Cisco Unified Communications Manager can only update the recorder that they are using; separate conferences are identified by the different conference identifiers (b-number). The conference chaining information can be obtained via Call Detailed Records (CDRs).

  Cisco Unified Communications Manager sends UPDATE messages to a recorder if the far-end call information changes. For a conference case, the far-end party address specifies the b-number. If the far-end b-number remains unchanged, Cisco Unified Communications Manager does not send the UPDATE messages to the recorder.

- Using Route List and/or Multiple Destination Addresses on a SIP Trunk for Multiple Recorders—When using a route list and/or multiple destination addresses on a SIP trunk for multiple recorders, the near-end and far-end recording calls of the same recording session can go to different recorders.

  If a Cisco Unified Communications Manager administrator configures a route list with multiple SIP trunks such that each SIP trunk points to a different recorder, Cisco Unified Communications Manager may not send the two recording calls of a recording session to the same SIP trunk, or to the same recorder. Depending on the selection algorithm that is provisioned in the route group, the likelihood of the two recording calls being sent to the same recorder may vary considerably. Similarly, Cisco Unified Communications Manager may not send the two recording calls to the same recorder if the administrator provisioned multiple IP addresses on a SIP trunk such that each IP address points to a different recorder. In this case, the calls get sent to the recorder that is randomly selected from the provisioned IP addresses.

  T configure Cisco Unified Communications Manager to support a recorder cluster configuration where a recording session may be redirected to another of the recorders in the cluster, configure a route list or provision multiple destinations on the recording SIP trunk.

GUI Changes

The following setting was added to the SIP Profile Configuration window:

Deliver Conference Bridge Identifier	Check this check box for the SIP trunk to pass the b-number that identifies the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require that this field be enabled. Checking this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

SIP OPTIONS

Description

In Cisco Unified Communications Manager, the SIP OPTIONS method allows a SIP trunk to track the status of remote destinations. By sending outgoing OPTIONS and checking the incoming response message, the SIP trunk knows whether remote peers are ready to receive a new request. The SIP trunk does not attempt to set up new calls to unreachable remote peers; this approach allows for quick failovers.

Cisco Unified Communications Manager uses SIP OPTIONS as a keep-alive mechanism on the SIP trunk. Cisco Unified Communications Manager periodically sends an OPTIONS request to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or returns a SIP error response, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address, depending on the configuration.

The OPTIONS request lies outside the context of a call; therefore, the request allows Cisco Unified Communications Manager to detect failures even if no calls are present on the SIP trunk. This approach allows any subsequent calls to be rerouted more quickly. The SIP OPTIONS method prevents calls from incurring large timeout and retry delays before the calls get rerouted.

Cisco Unified Communications Manager Administration Configuration Tips

The following configuration tips apply to Cisco Unified Communications Manager Administration when a SIP trunk is configured for OPTIONS:

- Configure a SIP profile to enable SIP OPTIONS. (Use the **Device > Device Settings > SIP Profile** menu option in Cisco Unified Communications Manager Administration.) Copy the Standard SIP Profile and rename the copy; for example, OPTIONS Profile. Check the **Enable OPTIONS Ping to monitor destination status for trunks with service type "None (Default)"** check box. SIP OPTIONS is disabled by default.
- From the SIP profile that you created, update the two request timers if necessary. One timer gets used when the SIP trunk is in service or partially in service; the second timer gets used when the SIP trunk is out of service. Cisco Unified Communications Manager initiates the SIP OPTIONS requests to the configured destination address(es) of the SIP trunk by using the configured transport protocol (for example, UDP or TCP).

Note When the request timers expire, Cisco Unified Communications Manager checks whether it has received responses to all previously sent OPTIONS requests. Cisco Unified Communications Manager does not send any new OPTIONS requests if it is still waiting for responses to previous OPTIONS requests. Thus, the system does not burden the network with multiple concurrent OPTIONS requests.

- From the SIP profile that you created, set the SIP OPTIONS retry timer and counter.
- Configure a SIP trunk (if one is not already configured). The trunk service type of the SIP trunk must specify None(default). Dynamic SIP trunks, such as Call Control Discovery, Extension Mobility Cross Clusters, and Intercompany Media Services, are not supported.
- Use Trunk Configuration to configure the destination information. Multiple destinations can be configured. If the destination address is configured as a host name (instead of a dotted IP address), and multiple addresses are returned, the system sends OPTIONS messages to the returned addresses until a response is received. If no response is received before all returned addresses have been exhausted, the SIP trunk gets marked as "target in down state."

Note For SIP trunks, Cisco Unified Communications Manager supports up to 16 IP addresses for each DNS SRV and up to 10 IP addresses for each DNS host name. The order of the IP addresses depends on the DNS response and may be identical in each DNS query. The OPTIONS request may go to a different set of remote destinations each time if a DNS SRV record (configured on the SIP trunk) resolves to more than 16 IP addresses, or if a host name (configured on the SIP trunk) resolves to more than 10 IP addresses. Thus, the status of a SIP trunk may change because of a change in the way a DNS query gets resolved, not because of any change in the status of any of the remote destinations.

- Assign the SIP profile that has OPTIONS Ping enabled to the SIP trunk.

When the destination of a SIP trunk includes or resolves to more than one IP address, call routing uses a random selection algorithm to select the destination IP address for the next call on a SIP trunk. If SIP OPTIONS is enabled for the trunk, the state information for the selected IP address determines whether to send the INVITE or advance to the next destination.

GUI Changes

The SIP Profile Configuration window supports the following new fields:

- Enable OPTIONS Ping to monitor destination status for trunks with service type "None (Default)"—Check this check box if you want to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or sends back a SIP error response such as 503 Service Unavailable or 408 Timeout, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address.

  If this check box is not checked, the SIP trunk will not keep track of the status of SIP trunk destinations.

  When checked, you can configure two request timers.

- Ping Interval for In-service or Partially In-service Trunks (seconds)—This field configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.

  Default is 60 seconds. Range is 5 to 600 seconds.

- Ping Interval for Out-of-service SIP Trunks (seconds)—This field configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if it fails to respond to OPTIONS, if it sends 503 or 408 responses, or if the Transport Control Protocol (TCP) connection cannot be established. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.

  Default is 120 seconds. Range is 5 to 600 seconds.

- Ping Retry Timer—This field specifies the maximum waiting time before retransmitting the OPTIONS request. Range is from 100 to 1000 milliseconds. Default is 500 milliseconds.

- Ping Retry Count—This field specifies the number of times that Cisco Unified Communications Manager resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low. Range is from 1 to 10. Default is 6.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

The following new alarms are generated for OPTIONS ping feature:

- SIPTrunkISV
- SIPTrunkOOS

- SIPTrunkPartiallyISV

For more information on OPTIONS ping alarm definitions, refer Serviceability - Alarms for Options Ping, page 63.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

The following security considerations exist for this feature.

SIP OPTIONS and Secure SIP Trunks

The SIP OPTIONS method supports secure SIP trunks for which the Transport Type setting specifies TLS in the SIP trunk security profile. Unlike other requests or responses (such as INVITE), Cisco Unified Communications Manager does not verify the X.509 Subject Name setting (configured in the SIP trunk security profile) for OPTIONS requests or responses. So, a remote destination can be marked as available based on OPTIONS request or response, but the call setup request (such as INVITE) may fail with a reason code 403 Forbidden. Misconfiguration of the X.509 Subject Name at either the Cisco Unified Communications Manager that sends the OPTIONS request or at the Cisco Unified Communications Manager that receives and responds to the OPTIONS request may cause this failure.

Consider the following two scenarios.

Scenario 1

Unified CM 1 sends an OPTIONS request over a SIP trunk to Unified CM 2 and receives a 200 OK response. The X.509 Subject Name in the SIP trunk security profile is misconfigured at Unified CM 2; therefore, Unified CM 2 gets marked as available at Unified CM 1. When the INVITE gets sent from Unified CM 1 to Unified CM 2, Unified CM 2 sends a 403 Forbidden message to Unified CM 1.

Scenario 2

Unified CM 1 sends an OPTIONS request over a SIP trunk to Unified CM 2 and receives a 200 OK response. Unified CM 1 marks Unified CM 2 as available, although the X.509 Subject Name in the SIP trunk security profile is misconfigured at Unified CM 1. In this case, the INVITE request from Unified CM 1 to Unified CM 2 fails.

SIP OPTIONS and Digest Authentication

When digest authentication is enabled for a SIP trunk (the Enable Digest Authentication check box is checked in the corresponding SIP trunk security profile), the remote destination gets marked as available upon receipt of a 401 (Unauthorized) response for the OPTIONS request. After receipt of a 401 response, OPTIONS is resent with the digest credentials; upon credential verification from the remote side, a 200 OK response is received for the OPTIONS request.

For an OPTIONS request where the SIP realm (upon receipt of an initial 401 response) or digest credentials are mismatched (remote side), any subsequent INVITE requests fail, even though the remote destination is marked as available.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

SIP Normalization and Transparency

Description

SIP trunks can connect to a variety of endpoints, including PBXs, gateways, and service providers. Each of these endpoints may implement the SIP protocol differently, causing a unique set of interoperability issues. SIP transparency and normalization allow Cisco Unified Communications Manager to seamlessly interoperate with a variety of PBXs and service providers. Normalization allows you to modify incoming and outgoing SIP messages at a protocol level on their way through Cisco Unified Communications Manager.Transparency allows Cisco Unified Communications Manager to pass headers, parameters, and content bodies from one call leg to the other.

You enable SIP Normalization by adding scripts to Cisco Unified Communications Manager and associating the scripts with a SIP trunk. You enable transparency through scripting rather than the graphical user interface.

Cisco Unified Communications Manager Administration Configuration Tips

Cisco Unified Communications Manager allows you to add or update scripts to the system and then associate them with one or more SIP trunks. The normalization scripts that you create allow you to preserver, remove, or change the contents of any SIP headers and content bodies, known or unknown. You upload a normalization script in Cisco Unified Communications Manager, by using the SIP Normalization Script Configuration window (**Device > Device Settings** .**SIP Normalization Script**).

You associate the script with a SIP trunk by configuring the Normalization Script fields on the Trunk Configuration window (**Device > Trunk**).

GUI Changes

A new window, SIP Normalization Script Configuration window, exists to allow administrators to add or update normalizaton scripts. Choose **Device > Device Settings** .**SIP Normalization Script**.

A new Normalizational Script group box on the Trunk Configuration window for SIP trunks contains three new fields: Name, Parameters, and Enable Trace check box. These fields allow you to associate a normalization script to a SIP trunk and to enable tracing. When you check the Enable Trace check box, the trace.output and trace.format API provided to the Lua scripter produces SDI trace that you can use to debug a script.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including script status and errors. Each device that has an associated script causes a new instance of these counters to be created.

Cisco Unified Communications Manager identifies the usage of and errors with SIP normalization scripts; that is, when the script gets opened and closed as well as when errors and resource warnings occur.

The system generates the following alarms:

- SIPNormalizationScriptOpened
- SIPNormalizationScriptClosed
- SIPNormalizationResourceWarning
- SIPNormalizationScriptError
- SIPNormalizationAutoResetDisabled

To debug scripts and call failures, you can enable tracing by checking the SDI Enable SIP Call Processing checkbox on the Trace Configuration window in Cisco Unified Serviceability. This option allows you to trace incoming and outgoing SIP messages before and after normalization.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Static Routing Enhancements (Run Route List on all nodes)

Description

Cisco Unified Communications Manager 8.5(1) supports SIP trunks and route lists that can simultaneously run in all nodes and Cisco Unified Communications Manager can randomly choose from any of the available SIP trunks or route lists that can reach a given node. The system can ensure that, over time and on average, all 16 nodes in the core cluster are used equally. This prevents system resources on some nodes from being idle while other nodes are dealing with an unsustainable call burden.

Following are the key features of the static routing enhancements:

- Route List is enhanced to have the option to run on every node.
- The generic SIP Trunk type is enhanced to have the option to run on every node.
- Cisco Unified Communications Manager Administration allows up to 16 sets of remote destination fields (16 IPv4 addresses, 16 IPv6 addresses, and 16 ports) or a single SRV to be configured on the generic SIP Trunk page.
- allows you to configure up to 16 sets of remote destination fields (16 IPv4 addresses/hostnames) on the generic H.323 non gatekeeper controlled ICT page.

Note For more information, refer to the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

Cisco Unified Communications Manager Administration Configuration Tips

GUI Changes

A new check box, Run On All Active Unified CM Nodes, is added to the Route List Configuration window and the Trunk Configuration window.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

BAT supports the following as part of the static routing enhancements:

- BAT supports the import/export of Run on All Nodes in Route List.
- BAT supports the import/export of Run on All Nodes in SIP Trunk.
- BAT supports the import/export of Run on All Nodes in H.323 Non Gatekeeper controlled ICT.
- BAT supports the import/export of Remote Destinations in SIP Trunk.
- BAT supports the import/export of Remote Destinations in H.323 Non Gatekeeper controlled ICT.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

AXL supports the configuration of 16 sets of remote destination fields (16 IPv4 addresses, 16 IPv6 addresses, 16 ports) on the generic SIP Trunk via the SipTrunk API.

AXL supports the configuration of 16 sets of remote destination fields (16 IPv4 addresses) on the H.323 ICT non-gatekeeper controlled API.

User Tips

No user tips exist for this feature.

Third-Party SIP Endpoints

Cisco Unified Communications Manager supports a variety of third-party SIP endpoints, which are configured in Cisco Unified Communications Manager Administration, Phone Configuration.

Cisco Unified Communications Manager requires user licenses. These licenses get configured in Cisco Unified Communications Manager Administration, License Configuration. When acquiring user licenses, the administrator purchases one user license, called user connect license (UCL), for each user.

License Configuration uses device license units (DLU). For example, if there are three generic desktop video endpoint users (3 UCLs), License Configuration would need 18 DLUs (3 UCL x 6 DLU = 18 DLU). For more information about licenses, refer to the following URL:

http://www.cisco.com/web/partners/downloads/partner/WWChannels/technology/ipc/downloads/uc_sol_og_ucl_final.pdf

When using Phone Configuration to add a third-party SIP endpoint, the following device phone types are available:

- Third-Party SIP Device (Advanced)—This eight-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies; this device requires 6 DLUs.
- Third-Party SIP Device (Basic)—This one-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies; this device requires 3 Device License Units (DLUs).
- Generic Desktop Video Endpoint—This SIP device supports video, security, configurable trust, and Cisco extensions; this device requires 6 DLUs. 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 requires 6 DLUs. 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 requires 6 DLUs. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.

Video and Interoperability Enhancements

Description

Cisco Unified Communications Manager 8.5 supports native or direct interoperability between Cisco video endpoints and 3rd party video endpoints such as Polycom. This means that Cisco Unified Communications Manager does not require a media gateway or conference bridge, such as Cisco Unified Video Conferencing (CUVC), for a simple point-to-point call between the supported endpoints.

Protocols and Deployments

Video and interoperability support the following protocols:

- SIP to SIP
- H323 to H323
- SIP to SIP Intercluster trunk (ICT) to SIP
- H323 to H323 ICT to H323
- SIP to H323 with or without ICT

For more information about limitations and special considerations of this features, see the "Limitations" section on page 43 and the *Cisco Unified Communications Solution Reference Network Design (SRND)*.

Video and interoperability support the following deployments:

- High-Definition interoperability for point-to-point calls
- Locations-based call admission control (CAC) only

- Presentation sharing and secure interop between TelePresence and third-party endpoints that support the Telepresence Interop Protocol (TIP)
- Multipoint calls involving Cisco TelePresence System (CTS), Cisco Unified Communications Manager, and third-party endpoints use Media transcoding Engine (MXE) and Cisco Unified Video Conferencing (CUVA)

For more information about supported deployments, see the *Cisco Unified Communications Solution Reference Network Design (SRND)*.

Cisco and Third-Party Endpoints Supported

Video and interoperability support the following endpoints:

- Cisco-certified third-party video endpoints
- Tandberg MXP 1000 (SIP and H323 support)
- Tandberg MXP 1700 (SIP and H323 support)
- Tandberg MXP 1000 (SCCP support)
- Tandberg MXP 6000 (SIP support)
- Video and interoperability support the following video endpoints with the Tandberg Video Conference Server (VCS):
  - Tandberg C-series
  - Tandberg EX90
- Cisco E20 (Tandberg E20)
- Cisco Unified Clients Services Framework (CSF) based clients, such as Cisco Unified Communication interface for Microsoft Office Communicator (CUCiMOC) or CUCiConnect (for example, Cisco WebEx)
- Cisco Unified Video Advantage (CUVA)
- Cisco Unified Personal Communicator (CUPC)
- Cisco Unified IP Phone 7985
- Cisco Unified IP Phone 9951 and 9971
- Cisco Unified IP Phone 8961 (requires CUVA)
- MeetingPlace Conference bridges, such as MP Hardware Media Switch (HMS) or Software Media Switch (SMS)

To find a Cisco-certified third-party device, go the following URL:

http://developer.cisco.com/web/partner/search

Perform the following steps:

1. Sign in to the Cisco Developer Network (CDN) (if applicable)
2. From the CDN main window, click the Technology Partners tab.
3. Click the Partner Search tab.
4. In the search box, enter the name of a 3rd party company (within all technologies) (for example, Polycom).
5. When the 3rd party company information displays, click the applicable links for more information.

Third-party devices get configured in Cisco Unified Communications Manager Administration, Phone Configuration. See Third-Party SIP Endpoints, page 40 for the list of supported device types.

For licensing requirements, see Third-Party SIP Endpoints, page 40.

Limitations

The following limitations apply:

- Advanced presentation sharing and security interoperability is supported only between two TelePresence Interop Protocol (TIP) capable endpoints.
- H239 presentation sharing and H235 security are supported only between two H323 endpoints.
- To ensure optimal resolution between the two endpoints, the protocol on the endpoints and the trunk should be identical; for example, SIP point-to-point endpoints connected by a SIP trunk.
- Locations-based CAC only for interoperability with TelePresence
- Ad hoc and Meet-Me conferencing support CUVC and MeetingPlace software media servers. Because the conferencing bridges support SCCP and the endpoints support SIP or H323, resolution may be limited to standard definition.
- Cisco Intercompany Media Engine (IME) is not supported between Cisco Unified Communications Manager endpoints and Telepresence.
- SRTP supported for audio channel only.

Cisco Unified Communications Manager Administration Configuration Tips

The following tips apply:

- No new configuration exists.
- SIP endpoint can be configured as 3rd Party SIP device (Advanced) or SIP Trunk.
- No change on Region and Location configuration; however, the administrator should ensure the bandwidth setting in Region configuration is enough for the desired resolution (for example, increase to 2Mbs for high-definition video call).

GUI Changes

Administrators configure the video endpoint, Cisco E20, in the Phone Configuration window of Cisco Unified Communications Manager Administration.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

The following tips apply:

- No difference or impact to user experience in making normal audio/video call.
- If video endpoints support high-definition format and use the same protocol, the user should see high-quality resolution.

Unified Communication OS Upgrade

Cisco Unified Communications Manager Release 8.5(1) uses a new version of the operating system. There should be no noticeable change in the operation of Cisco Unified Communications Manager, other than in direct upgrade path support and older server support.

Whisper Coaching

Silent call monitoring is a feature that allows a supervisor to discreetly listen to a conversation between an agent and a customer without allowing the agent to detect the monitoring session. Whisper coaching is an enhancement to silent call monitoring feature that allows supervisors to talk to agents during a monitoring session. This feature provides applications the ability to change the current monitoring mode of a monitoring call from Silent Monitoring to Whisper Coaching and vice versa.

To enable Whisper Coaching in the Cisco Unified Communications Manager Administration application, choose **Device > Phone**, locate the Cisco Unified IP Phone that you want to configure. Scroll to the Device Information Layout pane and set Built-in Bridge to **On** or **Default**. If Built-in Bridge is set to Default, in the Cisco Unified Communications Manager Administration application, choose **System > Service Parameter** and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (**Device - Phone**) pane and set Built-in Bridge Enable to **On**.

Windows 7 Support for RTMT

You can install the Real Time Monitoring Tool (RTMT), which works for resolutions 800*600 and above, on a computer that is running Windows 98, Windows XP, Windows 2000, Windows Vista, Windows 7 (32-bit), Windows 7 (64-bit) WOW64, or Linux with KDE and/or Gnome client.

Security

This section contains information on the following Security features and applications:

- Encryption to Analog Endpoints (sRTP), page 45
- Secure and Nonsecure Indication Tones, page 45

Encryption to Analog Endpoints (sRTP)

This feature enables you to create a secure SCCP connection for analog phones to a Cisco VG2xx Gateway. The gateway uses Transport Layer Security (TLS) with Cisco Unified Communications Manager for SCCP signaling communication and uses SRTP for voice communication. The existing Cisco Unified Communications Manager TLS functionality, including certificate management, is used for secure SCCP communication.

Phone Security Profile

To establish an encrypted connection to analog phones, you must create a Phone Security Profile for analog phones with the Device Security Mode parameter set to **Authenticated** or **Encrypted**. To create a Phone Security Profile, navigate to **System > Security Profile > Phone Security Profile** in Cisco Unified Communications Manager Administration.

For more information about creating a Phone Security Profile, see Chapter 6, "Configuring a Phone Security Profile," in the *Cisco Unified Communications Manager Security Guide*.

When you configure an analog phone attached to a Cisco VG2xx gateway, choose the secure analog profile you created for the **Device Security Profile** parameter. To configure the Device Security Profile parameter, navigate to **Device > Phone** in Cisco Unified Communications Manager Administration and scroll down to the Protocol Specific Information section for the phone you want to configure.

Certificate Management

For secure analog phones to function, you must import the same CA-signed certificate into Cisco Unified Communications Manager that is being used by the Cisco VG2xx Gateway. For more information about importing certificates, see Chapter 6, "Security," in the *Cisco Unified Communications Operating System Administration Guide*.

Secure and Nonsecure Indication Tones

The system plays secure and nonsecure indication tones on a protected phone to indicate whether a call is encrypted.

This section contains information on the following topics:

- Overview, page 45
- Supported Devices, page 46
- Important Information About Secure and Nonsecure Indication Tone, page 46
- Configuration Requirements, page 47

Overview

The secure indication tone gets played on a protected phone when the overall status of the call is protected, that is, when the system determines the call is encrypted. The tone denotes that the call is protected and that confidential information may be exchanged. The tone consists of three long beeps, and if the overall status of the call is protected, it begins to play on a protected phone as soon as the called party answers.

When the overall status of the call is not protected, the system plays nonsecure tone, which consists of six short beeps, on a protected phone.

Note Only callers on protected phones can hear secure and nonsecure indication tone. Callers on phones that are not protected never hear these tones.

Protected Devices

A protected device in Cisco Unified Communications Manager gets designated by configuration. You can configure only supported Cisco Unified IP Phones and MGCP E1 PRI gateways as protected devices in Cisco Unified Communications Manager.

Cisco Unified Communications Manager can also direct an MGCP IOS gateway to play secure and nonsecure tones when the system determines the protected status of a call.

You can make the following types of calls that clan use the secure and nonsecure indication tones:

- Intracluster IP-to-IP calls
- Intercluster calls that the system determines are protected
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI gateway

To determine which Cisco Unified IP Phone models that can be configured as protected devices, see the "Supported Devices" section on page 46.

Supported Devices

You can use Cisco Unified Reporting to determine which Cisco Unified IP Phone supports secure and nonsecure tones. From Cisco Unified Reporting, click **Unified CM Phone Feature List**. For the Feature, choose **Secure Tone** from the pull-down menu. The system displays a list of products that support the feature.

For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

Important Information About Secure and Nonsecure Indication Tone

This section provides information that pertains to the impact of using the secure-indication tone feature:

- Facts about protected devices:
  - You can configure phones that are running SCCP or SIP as protected devices.
  - Protected devices can call non-protected devices that are either encrypted or non-encrypted. In this case, the call will be non-protected and the nonsecure indication tone will play.
  - If a protected phone calls another protected phone, but the media is not encrypted, the call will not get dropped. In this case, the system plays nonsecure indication tone to phones on the call.
- For video calls, the system plays secure and nonsecure indication tones on protected de devices.

  Note For video calls, the user may first hear secure tone for the audio portion of the call and then nonsecure tone for overall nonsecure media.

- A lock icon that displays on a Cisco Unified IP Phone indicates that the media is encrypted, but does not necessarily mean that the phone has been configured as a protected device. However, the lock icon must be present for a protected call to occur.
- The following services and features are impacted:

  - Multi-line supplementary services such as call transfer, conference, and call waiting, are supported on protected phones. When the user invokes a supplementary service on a protected phone, the system plays secure or nonsecure tone to reflect the updated status of the call.
  - Cisco Extension Mobility and Join Across Line services are disabled on protected phones.
  - Shared-line configuration is not available on protected phones.
  - Hold/Resume and Call Forward All are supported for protected calls.
- Facts about MGCP E1 PRI gateways:
  - You must configure the MGCP gateway for SRTP encryption. Configure **mgcp package-capability srtp-package**.
  - The MGCP gateway must have an Advanced IP Services or Advanced Enterprise Services image (for example, c3745-adventerprisek9-mz.124-6.T.bin).
  - Protected status gets exchanged with the MGCP E1 PRI gateway by using proprietary FacilityIE in the MGCP PRI Setup, Alert, and Connect messages.
  - Cisco Unified Communications Manager plays the secure-indication tone only to the Cisco Unified IP Phone. A PBX in the network plays the tone to the gateway end of the call.
  - If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway is not encrypted, the call gets dropped.

Note For more information about encryption for MGCP gateways, refer to the *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for the version of Cisco IOS software you are using.

Configuration Requirements

You must configure the following items for the secure tone to play:

- On the Phone Configuration window, which you can navigate to by choosing **Device > Phone** in Cisco Unified Communications Manager Administration, configure the following items:
  - From the Softkey Template drop-down list in the Device Information portion of the window, choose **Standard Protected Phone**.

Note You must use a new softkey template without supplementary service softkeys for a protected phone.

  - For the **Join Across Lines** option (also in the Device Information portion of the window), choose **Off**.
  - Check the Protected Device check box (also in the Device Information portion of the window).
  - From the Device Security Profile drop-down list (in the Protocol Specific Information portion of the window), choose a secure phone profile that is already configured in the Phone Security Profile window (**System > Security Profile > Phone Security Profile).**
- Go to the Directory Number Configuration window that appears when you add a directory number from the Phone Configuration window. In the area of the Directory Configuration window that is called “Multiple Call/Call Waiting Settings on Device *DeviceName,”* set the following two options to a value of 1:
  - Maximum Number of Calls

  - Busy Trigger
- Choose **System > Service Parameters** in Cisco Unified Communications Manager Administration, select your server, and select the Cisco CallManager service. On the Service Parameter Configuration window, in the Feature - Secure Tone area, set the **Play Secure Indication Tone** option to **True** (it is False by default).
- If you are configuring a protected MGCP E1 PRI gateway, choose **Device > Gateway > Add New** in Cisco Unified Communications Manager Administration and select a supported gateway. Select **MCGP** as the protocol. When the Gateway Configuration window displays, be sure to include the following configuration choices:
  - Set **Global ISDN Switch Type** to **Euro**.
  - After you complete the rest of the MGCP Gateway configuration, click **Save**; then select the endpoint icon that appears to the right of subunit 0 in the window. The **Enable Protected Facility IE** check box displays. Check this check box.

    This allows the system to pass protected status of the call between Cisco Unified IP Phone endpoints and the protected PBX phones that are connected to the MGCP gateway.

Bulk Administration Tool

This section contains information on the following topics:

- End User CAPF Profile, page 48
- Update User Device Profile, page 49
- Mobility Profile, page 49

End User CAPF Profile

You can insert, delete, and export End User CAPF Profile details using the Users menu in the Bulk Administration Tool.

- Inserting End User CAPF Profile, page 48
- Deleting End User CAPF Profile, page 48
- Exporting End User CAPF Profile, page 49

Inserting End User CAPF Profile

You can insert End User CAPF Profile through Bulk Administration Tool. You can access the End User CAPF Profile Insert window by choosing **Bulk Administration > Users > End User CAPF Profile > Insert End User CAPF Profile**.

Deleting End User CAPF Profile

You can insert End User CAPF Profile through Bulk Administration Tool. You can access the End User CAPF Profile Insert window by choosing **Bulk Administration > Users > End User CAPF Profile > Delete End User CAPF Profile**.

Exporting End User CAPF Profile

You can export End User CAPF Profile through Bulk Administration Tool. You can access the End User CAPF Profile Insert window by choosing **Bulk Administration > Users > End User CAPF Profile > Export End User CAPF Profile**.

Note For more information on inserting, deleting, or exporting End User CAPF Profiles, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

Update User Device Profile

You can now update the user device profile (UDP) settings, such as changing or adding the device pool, or calling search space for a group of similar user device profiles, by using the Update UDP option.

You can locate the existing phone records by two methods:

- Using Query to Update UDPs, page 49
- Using Custom File to update UDPs, page 49

Using Query to Update UDPs

Choose **Bulk Administration > User Device Profiles > Update UDP > Query** to use a query to find and update the UDP.

Using Custom File to update UDPs

Choose **Bulk Administration > User Device Profiles > Update UDP > Custom File** to use a custom file to update the UDPs.

Note For more information on updating UDPs, including the update parameters, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

Mobility Profile

You can use Cisco Unified Communications Manager Bulk Administration (BAT) to add Mobility Profiles to remote destinations existing in the Cisco Unified Communications Manager database with a unique identity.

You have the following options for managing mobility profiles in BAT:

- Inserting Mobility Profile, page 49
- Deleting Mobility Profile, page 50
- Exporting Mobility Profile, page 50

Inserting Mobility Profile

You can insert Mobility Profile Choose **Bulk Administration > Mobility > Mobility Profile > Insert Mobility Profile** to insert Mobility Profiles in bulk.

Deleting Mobility Profile

Choose **Bulk Administration > Mobility > Mobility Profile > Delete Mobility Profile**. to delete Mobility Profiles in bulk.

Exporting Mobility Profile

Choose **Bulk Administration > Mobility > Mobility Profile > Export Mobility Profile**. to export Mobility Profiles in bulk.

Note For more information on working with Mobility Profiles in BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

Cisco Unified IP Phones and Video Endpoints

This section provides the following information:

- Assisted Directed Call Park, page 51
- Barge When Ringing Enhancement, page 51
- Call-Forward-All Upgrade for CTI New Call Event, page 52
- CAST Support for Cisco Unified IP Phones 8961, 9951, 9971 (SIP), page 52
- Cisco E20, page 53
- Gratuitous ARP Not Needed for Monitoring and Recording, page 53
- Handsfree, page 54
- Maximum ConfList Participants Shown, page 54
- Monitoring and Recording Support for Cisco Unified IP Phone 6901 and 6911, page 55
- Mute Support for Cisco Unified IP Phone 7906 and 7911, page 55
- Peer Firmware Sharing Update, page 56
- Plus Dialing, page 56
- Power Negotiation, page 56
- Remote Port Configuration and Automatic Port Synchronization, page 57
- Secure and Nonsecure Indication Tone, page 58
- Secure Extension Mobility, page 60
- Secure SIP Failover for SRST, page 60
- Single Sign On and SmartCard Authentication, page 61
- Voice-Quality Metrics Support for Cisco Unified IP Phones 6900 Series, page 61
- VPN Client, page 61

Assisted Directed Call Park

The Assisted Directed Call Park feature enables users to park a call by pressing only one button using the Direct Park feature. This requires administrators to configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.

This feature is supported on the following Cisco Unified IP Phones (SIP) for Cisco Unified Communications Manager 7.1(5) and later:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 9971G
- Cisco Unified IP Phone 9951G
- Cisco Unified IP Phone 8961G

Barge When Ringing Enhancement

A service parameter was added to Cisco Unified Communications Manager that allows a user (user B) to barge into a call not only when user A is connected to the call, but also when user A phone is still ringing out. When the barge is successful, user B also hears ringback tone. The feature is supported for the following phone models that support single-button barge:

- Phone models that support single-button barge through the cBarge feature by default, such as for the Cisco Unified IP Phone 9971
- Phone models that have been configured to invoke cBarge for the single-button Barge feature, such as for the Cisco Unified IP Phone 7975

The service parameter supports the following values:

- True—Allows a user to barge into a call when the phone is ringing or when the call is connected (the barger hears a ringback tone)
- False—Allows a user to barge only when a call is connected

This feature is supported on these Cisco Unified IP Phones (SCCP and SIP):

- Cisco Unified IP Phone 6901
- Cisco Unified IP Phone 6911

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6961
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified Wireless IP Phone 7925G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Call-Forward-All Upgrade for CTI New Call Event

With firmware release 9.0(3), information was added to the Computer Telephony Integration (CTI) new call event. The JTAPI and TAPI applications can now distinguish between an actual outgoing call and a call that is created when a user presses the call-forwarding softkey (CFwdALL or Forward All depending on the IP phone model), or presses the Forward All line button on the Cisco Unified IP Phone.

This upgrade applies only if the Call Forward All feature is invoked when the phone is on hook. If the phone is off hook, such as when a user lifts the handset or presses the speakerphone before invoking the Call Forward All feature, the CTI new call event will not provide the call-forward-all information.

These Cisco Unified IP Phones (SIP) support this feature:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

CAST Support for Cisco Unified IP Phones 8961, 9951, 9971 (SIP)

The Cisco Audio Session Tunnel (CAST) protocol establishes communication between the Cisco Unified Video Advantage (CUVA) and Cisco Unified IP Phones (SIP), which enables the CUVA to support video on the PC even if the IP phone does not have video capability.

When implemented on SIP phones, the CAST protocol enables communication with video applications when the PC is connected to the PC port on the phone.

The following phones support the CAST protocol:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Cisco E20

The Cisco E20 reinvents the desk phone by merging voice, video, and collaboration into one device. A highly scalable solution for enterprise mass deployment, users will immediately see the benefits of increased productivity and daily collaboration.

The Cisco E20 offers the following capabilities:

- Intuitive user interface and keypad for quick access to all IP phone and video services
- Familiar telephony features such as Hold, Transfer, Resume, and Conference
- Handset, headset (bluetooth), speakerphone flexibility
- Navigation cluster with select button
- Message waiting indicator/button
- 5 contextual softkeys
- USB picture frame
- High-resolution camera with integrated privacy shutter
- DVD quality, w448p video resolution
- 10.6" wide format LCD display with WXGA resolution
- Audio standards: MPEG4 AAC-LD, G.729ab, G.722, G.722.1, G.711
- Video standards and resolutions: H.264, H.263, and H.263+ from SIF up to w448p
- Bandwidth up to 1152 kbps

The Cisco E20 supports SIP.

Gratuitous ARP Not Needed for Monitoring and Recording

Administrators do not need to enable phones to accept Gratuitous ARP for the support of functions that monitor and record voice streams. These functions are active even if the Gratuitous ARP setting is disabled on Cisco Unified CM.

The following Cisco Unified IP Phones (SCCP and SIP) support this feature:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7942G

- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

Handsfree

The Bluetooth Handsfree Profile offers enhanced call-processing services (such as redial, reject, callerID, 3-way calling) while the user is connected to the Bluetooth application on the Cisco Unified IP Phone 9951 and 9971.

In firmware release 9.1(1), the existing Headset Profile has been replaced with the Handsfree Profile.

In addition to the Bluetooth qualified inter-operability requirements, the high-level call control, device management, and media service applications on the phone have been enhanced to support the Handsfree Profile. The Cisco Unified CM Administration displays a “Handsfree” option for Bluetooth Profiles.

These Cisco Unified IP Phones (SIP) support this feature:

- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Maximum ConfList Participants Shown

The conference participants list, ConfList, displays a maximum of 16 participants. Though users can add as many conference participants as the conference bridge supports, ConfList displays 16 participants only. As new participants join the conference, ConfList displays only the last 16 participants who have joined.

The following Cisco Unified IP Phones (SCCP and SIP) support this feature:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6961
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Monitoring and Recording Support for Cisco Unified IP Phone 6901 and 6911

The Monitoring and Recording feature allows you to monitor and record calls if desired. A supervisor using an encrypted phone can monitor an agent using an encrypted or unsecured phone. This feature can be set up for automatic recording of all calls or recording of calls on a per-call basis.

Users may receive audible alerts during call monitoring and recording. By default, the person who monitors the call and records it (if also configured) does not receive the audible alerts.

This features is supported on the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 6901
- Cisco Unified IP Phone 6911

Mute Support for Cisco Unified IP Phone 7906 and 7911

As of the firmware release 9.0(3) and Cisco Unified Communications Manager 6.1(5) or later, the Mute softkey can be used to mute and unmute active calls in off-hook, ringing, or connected state.

When users select Mute/Unmute, the following occurs:

- They receive an audible alert and a “Microphone Mute On” visual alert.
- When they press the softkey again, the softkey changes to Unmute, they receive an audible alert and a “Microphone Unmute Off” visual alert.

For the Mute softkey to be displayed in the phone:

- Cisco Unified CM 8.0 and later—Check the Enable Mute Feature check box in one of the following windows:
  - Phone Configuration (**Device > Phone**)
  - Enterprise Phone Configuration (**System > Enterprise Phone Configuration**)
  - Common Phone Profile (**Device > Device Settings > Common Phone Profile**)
- Earlier versions of Cisco Unified CM—Check the Enable Mute Feature check box in the Phone Configuration menu in Cisco Unified CM Administration.

This feature is supported on the following IP phones running the SCCP and SIP protocol:

- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

Peer Firmware Sharing Update

Peer Firmware Sharing enhances the firmware on phones in remote sites over low-speed WAN links and in enterprise LAN settings, by minimizing the firmware download traffic to the Cisco Unified Communications Manager servers and other load servers. In this release, this feature is enabled by default.

Plus Dialing

In this release, users can now press and hold the "*" key for 1 second to add a plus "+" sign as the first digit in a phone number for international dialing.

After the phone number includes the + sign, users can go into directories, such as received calls and call history, and select and dial the entry with the + sign without having to add digits for international calls.

This feature is supported on these Cisco Unified IP Phones (SCCP and SIP):

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6961
- Cisco Unified IP Phone 6901
- Cisco Unified IP Phone 6911

Power Negotiation

The Power Negotiation feature enables phones to connect to switches that do not support power negotiation, and enables the phone to power up the accessories up to 12.9 watts.

Power Negotiation is Enabled by default, so the phone will use Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) protocols to negotiate power.

Cisco recommends that Power Negotiation must always be enabled (default) when connecting to a switch that supports power negotiation. If disabled, the switch may disconnect power to the phone.

For switches that do not support power negotiation, disable Power Negotiation before you power up accessories over Power over Ethernet (PoE). With Power Negotiation Disabled, the phone can power accessories up to 12.9W.

When Power Negotiation and CDP are disabled, the phone can power accessories up to 15.4W.

Note To prevent inadvertent power shut off to the phone, do not disable the Power Negotiation feature when the phone is connected to a switch that supports power negotiation.

Power Negotiation is enabled by default. To change the setting of Power Negotiation to Disabled, select Disabled in the Power Negotiation drop-down list box in the Phone Configuration window, Product Specific Configuration.

The Power Negotiation feature is supported on the following phones that are running SIP:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Remote Port Configuration and Automatic Port Synchronization

Remote Port Configuration

The Remote Port Configuration feature allows the administrator to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager Administration. This enhances the performance for large deployments with specific port settings. The setting in Unified CM allows the administrator to override the local (manual) setting on the phone.

Automatic Port Synchronization

When the Cisco Unified CM administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP phone remotely, loss of packets can occur if one port is slower than the other.

The Automatic Port Synchronization feature synchronizes the ports to the lowest speed among the two ports, which eliminates packet loss. When automatic port synchronization is enabled, it is recommended that both ports be configured for autonegotiate. If one port is enabled for autonegotiate and the other is at a fixed speed, the phone synchronizes to the fixed port speed.

Note If both the ports are configured for fixed speed, the Automatic Port Synchronization feature is ineffective.

Note The Remote Port Configuration and Automatic Port Synchronization features are compatible only with IEEE 802.3AF Power of Ethernet (PoE) switches. Switches that support only Cisco Inline Power are not compatible. Enabling this feature on phones that are connected to these types of switches could result in loss of connectivity to Cisco Unified CM, if the phone is powered by PoE.

These two features are supported on the following phones that are running SCCP or SIP:

- Cisco Unified IP Phone 6901 (no PC port) (supports Remote Port Configuration only)
- Cisco Unified IP Phone 6911 (same as 6921, 6941, 6961)
- Cisco Unified IP Phone 6921 (no Gig support 1000 Full)
- Cisco Unified IP Phone 6941 (no Gig support 1000 Full)
- Cisco Unified IP Phone 6961 (no Gig support 1000 Full)
- Cisco Unified IP Phone 7906G (no PC port) (supports Remote Port Configuration only)
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Secure and Nonsecure Indication Tone

With firmware release 9.0(3), the secure indication tone functionality was updated, and the nonsecure indication tone was added to the Secure and Nonsecure Indication Tone feature for the Cisco Unified IP Phones. The 8.0(3) release of Cisco Unified Communications Manager (Unified CM) is a requirement for these changes to function.

If phone is configured as secure (encrypted and trusted) in Unified CM, it can be given a “protected” status (which is separate from the status a call). After that if desired, the protected phone can be configured to play an indication tone at the beginning of a call:

- Protected Device—To change the status of a secure phone to protected, check the “Protected Device” check box in Cisco Unified Communications Manager Administration (**Device > Phone > Phone Configuration**).
- Play Secure Indication Tone—To enable the protected phone to play a secure or nonsecure indication tone, set the “Play Secure Indication Tone” to True. (The default is False.) You set this option in Cisco Unified Communications Manager Administration (**System > Service Parameters**). Select the server and then the Unified CM service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. (The default is False.)

Only protected phones hear secure or nonsecure indication tones. (Nonprotected phones never hear tones.) Because the condition for playing the secure indication tone is now based on the overall secure status of the call end to end and not the protected status of the phone, users hear a tone between a protected phone and a nonprotected phone if the Secure Real-Time Transfer Protocol (SRTP) or Real-Time Protocol (RTP) is established.

If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected phone plays the appropriate tone.

A protected phone plays a tone or not under these circumstances:

- When the option to play a tone, "Play Secure Indication Tone," is enabled (True):
  - When end-to-end secure media is established through the Secure Real-Time Transfer Protocol (SRTP) and the call status is secure, the phone plays the secure indication tone (three long beeps with brief pauses).
  - When end-to-end nonsecure media is established through the Real-Time Protocol (RTP) and the call status is nonsecure, the phone plays the nonsecure indication tone (six short beeps with brief pauses). (This capability is a change with this release.)
- When the Play Secure Indication Tone option is disabled (False), no tone is played.

These changes were also made with this release:

  - Users can invoke supplementary services, such as Transfer or Conference, from protected phones without a software limitation.
  - In the past if calls were transferred from a protected phone to another protected phone with RTP established, the call would be dropped. Now users hear a secure or nonsecure indication tone instead of the call being dropped.

The Secure and Nonsecure Indication Tone feature is supported on these IP phones running the SCCP and SIP protocol:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 9971

- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 8961

Secure Extension Mobility

The Cisco Extension Mobility HTTPS Support feature ensures that when communications are exchanged between a Cisco Unified IP Phone service and other applications, that the communications use the HTTPS protocol to ensure that the communications are secure. Users must log into the Cisco Unified CM applications by providing their authentication information. Their credentials are encrypted after the communication protocol changes to HTTPS.

When a visiting Extension Mobility (EM) application fails to locate a user's identification in the local database, the following occurs:

6. Cisco Extension Mobility Cross Cluster (EMCC) sends a request to the local EM service to determine the home cluster of that user (the cluster which owns the user's identification, and which can handle the EM login).
7. The visiting EM service sends a user identification message over HTTPS to all the remote clusters added in the local database.
8. The visiting EM service then parses the response received from the home cluster to get the list of device profiles associated with that user.
   - All further communication between the visiting EM service and home EM service takes place over HTTPS.
   - Similarly, visiting logout requests are also sent from the home EM service to the visiting EM service over HTTPS.

Note Configure Cisco Extension Mobility on Cisco Unified IP Phones before configuring EMCC.

The Cisco Extension Mobility HTTPS Support feature is supported on the following IP phones (SIP):

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Secure SIP Failover for SRST

Firmware release 9.1(1) provides security support for calls on a Cisco Unified IP Phone running the Session Initiation Protocol (SIP) protocol. Secure SIP Failover for SRST enables calls to remain secure once the call fails over to Survivable Remote Site Telephony (SRST) from Cisco Unified Communications Manager.

The Secure SIP Failover for SRST feature enables VoIP calls that fail over to SRST devices to provide secure and encrypted transport using SIP. These voice calls originate from IP phones running the SIP protocol. In addition, this feature enables the user to verify that the call is still secure by the Lock icon that remains on the phone display.

Depending on the security configuration security settings are configured, the SRST supports RTP and SRTP media connections on the IP phone.

The system administrator configures SRST on a Cisco router to allow SIP phones to register to SRST using SIP/User Datagram Protocol (UDP), SIP/TCP, and SIP/Transfer Layer Security (TLS)/TCP.

For firmware release 9.1(1), when a SIP phone is in a secure call that fails over to SRST from Unified CM, the user will continue to see the a Lock icon will be displayed to indicate that the call is secure.

When IP phones register to the SRST, if all segments of the call are SIP phones, then all the supplementary features are supported—Conference, Transfer, Blind Transfer, and Call Forward. If the segments of the call are both SIP and SCCP phones, then only basic call is supported.

This feature is supported on the following SIP phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Single Sign On and SmartCard Authentication

If the Single Sign-On feature is configured by the system administrator, users can access their Cisco Unified CM User Options web page without having to sign in.

These Cisco Unified IP Phones (SIP) support this feature:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Voice-Quality Metrics Support for Cisco Unified IP Phones 6900 Series

The Mean Opinion Score (MOS) for Listening Quality (LQK) algorithm, is a Cisco-proprietary, voice quality metric that is used to calculate MOS for LQK scores. These scores are objective estimates of the Mean Opinion Score (MOS) for Listening Quality (LQK) that rates from 5 (excellent) to 1 (bad). Scores are based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream.

The following phone models support the MOS LQK Voice-Quality metrics:

- Cisco Unified IP Phone 6911
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6961

VPN Client

The VPN Client feature establishes a virtual private network (VPN) connection on your phone using the Secure Sockets Layer (SSL). The VPN connection is used when a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager must cross untrusted networks.

The status of Auto-Detect Network Connection determines if a VPN connection is possible:

- If Auto-Detect Network Connection is disabled, a VPN connection is possible. The Sign In screen appears, and you are prompted for credentials based on the authentication method that your system administrator configured on your phone. (On the phone in the Applications > VPN window, you can toggle the VPN Enabled field to On or Off to turn on or off the phone's ability to attempt a VPN connection.)

- If Auto-Detect Network Connection is enabled, you cannot connect through VPN, so the Sign In screen does not appear, and you are not prompted for credentials.

The system administrator determines if the user's phone should be configured with the VPN functionality and enables the VPN Client feature.

These Cisco Unified IP Phones (SIP) support this feature:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Cisco Unified Serviceability

This section contains information on the following topics:

- Audit Log Support for Cisco Unity Connection, page 62
- Serviceability - Alarms for Options Ping, page 63
- Serviceability - Alarms for SIP Normalization and Transparency, page 68
- Serviceability - Alarms for SIP Normalization and Transparency, page 68
- Serviceability - Alarms for Single Sign On and SmartCard Authentication, page 81
- Serviceability - Enhanced Reason Codes for Device De-Reg, page 84
- Serviceability - Session Manager Edition (SME), page 87
- Default Settings for Alarm Configuration Settings, page 92
- New Cisco Unity Connection Alerts, page 92
- New CDR Field for Hunt List Support, page 94
- SNMP MIBs, page 94
- Logging On to CAR, page 99
- Configuring the Trunk, page 99
- Configuring Trunk Utilization Reports, page 100
- Cisco Dialed Number Analyzer Server, page 102

Audit Log Support for Cisco Unity Connection

With audit logging, configuration changes to the Cisco Unity Connection system gets logged in separate log files for auditing.

The following components generate audit events for Cisco Unity Connection:

- Command-Line Interface, page 63
- Cisco Unity Connection Administration, page 63
- Cisco Personal Communications Assistant (Cisco PCA), page 63
- Cisco Unity Connection Serviceability, page 63
- Cisco Unity Connection Clients that Use the Representational State Transfer APIs, page 63

Command-Line Interface

All commands issued via the command-line interface are logged (for both Cisco Unified Communications Manager and Cisco Unity Connection).

Cisco Unity Connection Administration

Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts).
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony.
- Task management (enabling or disabling a task).
- Bulk Administration Tool (bulk creates, bulk deletes).
- Custom Keypad Map (map updates)

Cisco Personal Communications Assistant (Cisco PCA)

The Cisco Personal Communications Assistant client logs the following events:

- User logging (user logins and user logouts).
- All configuration changes made via the Messaging Assistant.

Cisco Unity Connection Serviceability

Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

Cisco Unity Connection Clients that Use the Representational State Transfer APIs

Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface (CUPI).

For Cisco Unity Connection, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role. You can also remove the Audit Administrator role from this account.

The Audit Administrator role in Cisco Unity Connection provides the ability to view, download and delete audit logs in Cisco Unified Real Time Monitoring Tool.

For information on roles and users in Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

For a description of the settings that you can configure for audit log configuration, refer to the *Cisco Unified Serviceability Administration Guide*.

Serviceability - Alarms for Options Ping

Cisco Unified Communications Manager SIP OPTIONS allows a SIP trunk to track the status of remote destinations.

Note With Cisco Unified Communications Manager Release 8.5, you can turn on Option Ping, but you will not receive an email after Cisco Unified Communications Manager cannot reach a particular SIP trunk destination.

The following new alarms are generated for OPTIONS ping:

- SIPTrunkISV, page 64
- SIPTrunkOOS, page 64
- SIPTrunkPartiallyISV, page 66

SIPTrunkISV

All remote peers are available to handle calls for this SIP trunk.

This alarm indicates that all the remote peers are available to handle the calls for this SIP trunk. For each peer, the alarm provides the resolved IP address and port number, and hostname or SRV (if configured on SIP trunk).

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

SIP Trunk Name(String)

Available remote peers for this SIP trunk(String)

Recommended Action

Notification purpose only; no action is required.

SIPTrunkOOS

All remote peers are out of service and unable to handle calls for this SIP trunk.

This alarm provides the list of unavailable remote peers, where each peer is separated by semicolon. It also provides the reason code received by the SIP trunk, in response to an Options request sent to remote peer. For each peer, the alarm provides the hostname or SRV (if configured on SIP trunk), resolved IP address, port number, and reason code in the following format:

ReasonCodeType=ReasonCode.

The ReasonCodeType depends on a SIP response from the remote peer as defined in SIP RFCs (remote), or depends on a reason code provided by Unified CM (local).

The examples of possible reason codes include:

- Remote = 503 ("503 Service Unavailable" a standard SIP RFC error code)
- Remote = 408 ("408 Request Timeout" a standard SIP RFC error code)
- Local = 1 (request timeout)
- Local = 2 (local SIP stack is unable to create a socket connection with remote peer)
- Local = 3 (DNS query failed)

  For Local=3, IP address in the alarm is represented as zero, and when DNS SRV is configured on SIP trunk then the port is represented as zero.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

SIP Trunk Name(String)

Unavailable remote peers with Reason Code(String)

Recommended Action

- For Remote = 503, the possible reasons include:
  - Route/SIP trunk for originating side does not exist on remote peer. If remote peer is Unified CM, add a new SIP trunk in Unified CM Administration for the remote peer (**Device > Trunk**) and ensure the Destination Address and Destination Port fields are configured to point to the originating host (the originating host is the same node on which this alarm was generated).
  - Route/SIP trunk for originating side does exist on remote peer but the port is either used for a SIP phone or a different SIP trunk. If remote peer is Unified CM, in the Unified CM Administration for the remote peer (**Device > Trunk**), ensure the Destination Port on the originating side is configured to be the same as the incoming port on the terminating side SIP Trunk Security Profile.
  - Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.
- For Remote = 408, the possible reason includes:

  - Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.

- For Local = 1, the possible reason could be that no responses are received for OPTIONS request after all retries, when UDP transport is configured in the SIP trunk Security Profile assigned to the SIP trunk on the originating side.

  To fix this issue, perform the following steps:

  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools > Control Center (Feature Services)** and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device > Trunk**, and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command `utils network ping <remote peer>` at the originating side.

- For Local = 2, the possible reason could be that Unified CM is unable to create the socket connection with remote peer.

  To fix this issue, perform the following steps:

  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools > Control Center (Feature Services)** and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device > Trunk** and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command `utils network ping <remote peer>` at the originating side.

- For Local = 3, the possible reason could be that DNS server is not reachable, or DNS is not properly configured to resolve the hostname or SRV which is configured on the local SIP trunk.

  To fix this issue, perform the following steps:

  a. In the OS Administration, choose **Show > Network** and verify whether the DNS details are correct. If it is not correct, configure the correct DNS server information by using the CLI command `set network dns primary`.
  b. Check the network connectivity with DNS server by using the CLI command `utils network ping <remote peer>`, and ensure the DNS server is properly configured.

SIPTrunkPartiallyISV

Some of the remote peers are not available to handle calls for this SIP Trunk.

The alarm provides a list of available remote peers and a list of unavailable remote peers, where each peer is separated by semicolon. For each available peer, the alarm provides resolved IP address and port number, and hostname or SRV (if configured on SIP trunk). For each unavailable peer, the alarm provides the hostname or SRV (if configured on SIP trunk), resolved IP address, port number, and reason code in the following format: ReasonCodeType=ReasonCode.

The ReasonCodeType depends on a SIP response from remote peer as defined in SIP RFCs (Remote), or depends on a reason code provided by Unified CM (Local).

The examples of possible reason codes include:

- Remote = 503 ("503 Service Unavailable" a standard SIP RFC error code)
- Remote = 408 ("408 Request Timeout" a standard SIP RFC error code)
- Local = 1 ("Request Timeout")
- Local = 2 (local SIP stack is unable to create a socket connection with remote peer)
- Local = 3 (DNS query failed)

  For Local=3, IP address in the alarm is represented as zero, and when DNS SRV is configured on SIP trunk then port is represented as zero.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

SIP Trunk Name(String)

Unavailable remote peers with Reason Code(String)

Available remote peers for this SIP trunk(String)

Recommended Action

The available peer list is for notification purposes only; no action is required. For unavailable peers, the following corrective action should be taken.

- For Remote = 503, the possible reasons are:
  - Route/SIP trunk for originating side does not exist on remote peer. If remote peer is Unified CM, add a new SIP trunk in Unified CM Administration for the remote peer **(Device > Trunk)** and ensure the Destination Address and Destination Port fields are configured to point to the originating host (the originating host is the same node on which this alarm was generated). Also ensure the new SIP trunk has the incoming port in associated SIP Trunk Security Profile configured to be the same as originating side SIP Trunk destination port.
  - Route/SIP trunk for originating side does exist on remote peer but port is either used for SIP phone or other SIP trunk. If remote peer is Unified CM, in the Unified CM Administration for the remote peer (**Device > Trunk**), ensure the incoming port in associated SIP Trunk Security Profile is configured to be same as originating side SIP Trunk destination port.
  - Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.
- For Remote = 408, the possible reason includes:

  - Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.

- For Local = 1, the possible reason could be that no responses are received for OPTIONS request after all retries, when UDP transport is configured in SIP Trunk Security Profile assigned to the SIP trunk on originating side.

  To fix this issue, perform the following steps:

  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools > Control Center (Feature Services)** and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device > Trunk**, and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command `utils network ping <remote peer>` at the originating side.

- For Local = 2, the possible reason could be that Unified CM is unable to create the socket connection with remote peer.

  To fix this issue, perform the following steps:

  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools > Control Center (Feature Services)** and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device > Trunk**, and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command `utils network ping <remote peer>` at the originating side.

- For Local = 3, the possible reason could be that DNS server is not reachable, or DNS is not properly configured to resolve the hostname or SRV which is configured on the local SIP trunk.

  To fix this issue, perform the following steps:

  - In the OS Administration, choose **Show > Network**, and verify that the DNS Details are correct. If it is not correct, then configure the correct DNS server information by using the CLI command `set network dns primary`.
  - Check the network connectivity with DNS server by using the CLI command `utils network ping <remote peer>`, and ensure the DNS server is properly configured.

Serviceability - Alarms for SIP Normalization and Transparency

Cisco Unified Communications Manager identifies the usage of and errors with SIP normalization scripts; that is, when the script gets opened and closed as well as when errors and resource warnings occur.

The following new alarms are generated for SIP Normalization and Transparency:

- SIPNormalizationScriptOpened, page 69
- SIPNormalizationScriptClosed, page 69
- SIPNormalizationAutoResetDisabled, page 70
- SIPNormalizationResourceWarning, page 71

- SIPNormalizationScriptError, page 73

SIPNormalizationScriptOpened

Cisco Unified CM opened the script for the SIP device.

The normalization script for the indicated SIP device has been successfully loaded, initialized, and activated on Cisco Unified CM.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

In Use Memory(UInt)

Recommended Action

Notification purposes only; no action is required.

SIPNormalizationScriptClosed

Cisco Unified CM has closed the script for the SIP device. The script is closed at one of the following conditions:

- The indicated device (SIP trunk) was reset manually or automatically.
- The trunk was deleted manually.
- Due to script error or resource error or internal error.

When the script is closed, Cisco Unified CM will not invoke normalization script message handlers for the indicated SIP device.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Reason Code(Enum)

Reason Text(String)

Additional Information(String)

Enum Definitions - Reason Code

Value	Definition
1	DeviceResetManually—The associated device is reset manually using Cisco Unified CM Administration.
2	DeviceResetAutomatically—The associated device is reset automatically; the reset was triggered by an execution error in the script.
3	DeviceDeleted—The associated device is manually deleted in Cisco Unified CM Administration.
4	ScriptDisassociated—A configuration change occurred in Cisco Unified CM Administration and the script is no longer associated with the device.
5	ScriptInfoChanged—A change in the script logic occurred or a change to one or more fields on the SIP Normalization Script Configuration window in Cisco Unified CM Administration occurred.
6	ScriptError—An error occurred in the script; check for the occurrence of SIPNormalizationScriptError alarm and perform the recommended actions described to correct the script error.

Recommended Action

This alarm serves as a notification of the script closure, if the alarm has occurred due to a SIP trunk maintenance window or any other expected reason for the script to close. If this alarm is unexpected, check for an occurrence of the SIPNormalizationScriptError alarm and refer to the specific action based on the reason code identified in the SIPNormalizationScriptError alarm.

SIPNormalizationAutoResetDisabled

An error occurred repeatedly and Cisco Unified CM disabled the script.

The script failed due to execution errors that occurred three times within a 10 minute period. As a result, the normalization script for the indicated SIP device has been disabled. Cisco Unified CM do not attempts to automatically reset either the script or the device for the purpose of recovering the script.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Script Type(String)

Reason Code(Enum)

Reason Text(String)

Additional Information(String)

Enum Definitions - Reason Code

Value	Definition
1	ScriptResetDisabled—The system has automatically reset the script three times within a 10 minute period due to script execution errors; on the fourth occurrence of this error, Cisco Unified CM disabled the script.
2	TrunkResetDisabled—The system has automatically reset the trunk three times within a 10 minute period due to script execution errors; on the fourth occurrence of this error, Cisco Unified CM disabled the script.

Recommended Action

Notification purposes; examine the information and perform the recommended actions in the SIPNormalizationScriptError alarm, which should have been issued before this alarm.

SIPNormalizationResourceWarning

The normalization script has exceeded an internal resource threshold.

The normalization script for the indicated SIP device has exceeded an internal threshold for resource consumption. This alarm can occur for memory consumption, or when the script is close to exceeding the configured allowance of Lua instructions. When the amount of memory (as defined in the Memory Threshold field) or the number of Lua instructions utilized by this script (as defined by the Lua Instruction Threshold) exceeds an internal threshold, this alarm is triggered.

Examples

1. If the memory threshold is set to 100 KB and the internal threshold is 80%, this alarm will occur when this script has consumed 80 KB of memory. The internal threshold is not configurable and may fluctuate from Cisco Unified CM release to release.
2. If the Lua Instruction Threshold is set to 2000 and the internal threshold is 50%, this alarm will occur when the script has executed 1000 Lua instructions.

This alarm warns that the resources (either memory or Lua instructions) have crossed an internal mark, where investigation into the consumption of those resources may be advisable to ensure the health of the script.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Routing List

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Script Function(String)

Script Type(String)

Reason Code(Enum)

Reason Text(String)

In Use Memory(UInt)

Memory Threshold (UInt)

In Use Lua Instructions(UInt)

Lua Instruction Threshold(UInt)

Enum Definitions - Reason Code

Value	Definition
1	InternalLuaInstructionsThreshold—The script exceeds the internal threshold for the number of Lua instructions.
2	InternalMemoryThreshold—The script exceeds the internal threshold for script memory usage.

Recommended Action

1. Examine the thresholds (Memory Threshold and Lua Instruction Threshold) configured in the SIP Normalization Script Configuration window.
2. Evaluate if the thresholds can be increased (take into consideration the CPU resources and memory when deciding to increase these values), or examine the script to determine if the message handlers can be written more efficiently to reduce the number of instructions in the script.
3. Examine the script for logic errors. If the script is functioning normally but contains extensive logic, consider increasing the value in the Lua Instruction Threshold field. Be aware that more computing resources will be consumed as a result. You can also examine SDI trace files for additional details about this resource condition. For scripts provided by Cisco, contact the Cisco Technical Assistance Center (TAC).
4. Investigate and correct the resource issue before the script closes. When the values that have been configured in the Memory Threshold field, or Lua Instruction Threshold field or both the fields on the SIP Normalization Script Configuration window are met, the script closes and the SIPNormalizationScriptClosed alarm also occurs. For additional information when troubleshooting, check the SIP Normalization counter, MemoryUsagePercentage to learn the current resource usage.

SIPNormalizationScriptError

Description

A script error occurred.

Explanation

Cisco Unified CM encountered an error during loading, initializing, or during execution of the SIP normalization script for the indicated SIP device. If the error was due to a resource issue, the SIPNormalizationResourceWarning alarm will also be issued. The Configured Action shown in this alarm may differ from the Resulting Action shown in this alarm because certain errors, such as those occurring during loading or initialization, cannot be configured. If the script closes three times within a 10 minute window due to errors, Cisco Unified CM will follow the configured action three times; on the fourth occurrence of the error, Unified CM disables the script and issues the SIPNormalizationAutoResetDisabled alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Script Function(String)

Script Type(String)

Error Code(Enum)

Error Code Text(String)

Error Message(String)

Configured Action(String)

Resulting Action(String)

In Use Memory(UInt)

Memory Threshold(UInt)

In Use Lua Instructions(UInt)

Lua Instruction Threshold(UInt)

Enum Definitions - Reason Code

Value	Definition
1	LoadError —The script failed to load either due to a syntax error in the script or a resource error; check the Recommended Actions for instructions.
2	InitializationError—The script encountered a failure while initializing either due to a syntax error in the script or a resource error; check the Recommended Actions for instructions.
3	ExecutionError—The script encountered a failure during execution; check the Recommended Actions for instructions.
4	InternalError—The system encountered an unexpected condition during execution; check the Recommended Actions for instructions.

Recommended Action

1. Examine SDI trace files for details regarding the error such as function calls and the call ID. This will help you to troubleshoot the error.
2. Examine the script for syntax or logic errors; for scripts provided by Cisco, contact the Cisco Technical Assistance Center (TAC). If the error was due to a resource issue, the SIPNormalizationResourceWarning alarm will also be issued. Check the SIPNormalizationResourceWarning alarm for additional information and recommended actions.

Serviceability - Perfmon Counters for SIP Normalization and Transparency

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including initialization errors, runtime errors, and script status. Each device that has an associated script causes a new instance of these counters to be created. Table 3 provides information on the Cisco SIP Normalization counters.

Table 3 Cisco SIP Normalization

Display Name	Description
DeviceResetAutomatically	This counter indicates the number of times that Cisco Unified CM automatically resets the device (SIP trunk). The device reset is based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. When the device (SIP trunk) is reset due to script errors, the counter value increments. This count restarts when the device is reset manually.
DeviceResetManually	This counter indicates the number of times that the device (SIP trunk) is reset manually in Cisco Unified Communications Manager Administration or by other methods, such as AXL. When the device associated with a script is reset due to configuration changes, the counter value increments. The counter restarts in the following situations: • The SIP trunk is deleted. • The script on the trunk gets changed or deleted. • Cisco Unified Communications Manager restarts.
ErrorExecution	This counter represents the number of execution errors that occurred while the script executed. Execution errors can occur while a message handler executes. Execution errors can be caused by resource errors, an argument mismatch in a function call, and so on. When an execution error occurs, Cisco Unified CM performs the following actions: • Automatically restores the message to the original content before applying additional error handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in Cisco Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the trunk. This counter increments every time an execution error occurs. This counter provides a count from the most recent trunk reset that involved a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the script again.

Table 3 Cisco SIP Normalization (continued)

Display Name	Description
ErrorInit	This counter represents the number of times a script error occurred after the script successfully loaded into memory, but failed to initialize in Cisco Unified CM. A script can fail to initialize due to resource errors, an argument mismatch in a function call, the expected table was not returned, and so on. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the trunk. This counter increments every time an initialization error occurs. This counter provides a count from the most recent trunk reset that was accompanied by a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the script again. When the error occurs during initialization, Cisco Unified CM automatically disables the script.
ErrorInternal	This counter indicates the number of internal errors that occurred while the script executed. Internal errors are very rare. If the value in this counter is higher than zero, a defect exists in the system that is not related to the script content or execution. Collect SDI traces and contact the Technical Assistance Center (TAC).
ErrorLoad	This counter represents the number of times a script error occurred when the script loaded into memory in Cisco Unified Communications Manager. A script can fail to load due to memory issues or syntax errors. Check the SIPNormalizationScriptError alarm for details. Check the script syntax for errors, upload the corrected script as needed, and reset the trunk. This counter increments every time a load error occurs. This counter provides a count from the most recent trunk reset that was accompanied by a script configuration change. (A device reset alone will not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment even after you fix the script problem, examine the script again.
ErrorResource	This counter indicates whether the script encountered a resource error. Two kinds of resource errors exist: exceeding the value in the Memory Threshold field and exceeding the value in the Lua Instruction Threshold field. (Both fields display on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration.) If either condition occurs, Cisco Unified Communications Manager immediately closes the script and issues the SIPNormalizationScriptError alarm. If a resource error occurs while the script loads or initializes, the script is disabled. If a resource error occurs during execution, the configured system resource error recovery action is taken. (The setting of the System Resource Error Recovery Action field on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration defines this action.)

Table 3 Cisco SIP Normalization (continued)

Display Name	Description
MemoryUsage	This counter specifies the amount of memory, in bytes, that the script consumes. This counter increases and decreases to match the amount of memory that the script uses. This count gets cleared when the script closes (because a closed script does not consume memory) and restarts when the script opens (gets enabled). A high number in this counter indicates a resource problem. Check the MemoryUsagePercentage counter and the SIPNormalizationResourceWarning alarm, which occur when the resource consumption exceeds an internally set threshold.
MemoryUsagePercentage	This counter specifies the percentage of the total amount of memory that the script consumes. The value in this counter is derived by dividing the value in the MemoryUsage counter by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying the result by 100 to arrive at a percentage. This counter increases and decreases in accordance with the MemoryUsage counter. This count gets cleared when the script closes (because closed scripts do not consume memory) and restarts when the script opens (gets enabled). When this counter reaches the internally controlled resource threshold, the SIPNormalizationResourceWarning alarm is issued.
MessageRollback	This counter indicates the number of times that the system automatically rolled back a message. The system rolls back the message by using the error handling that is specified in the Script Execution Error Recovery Action field in the SIP Normalization Script Configuration window in Cisco Unified CM Administration. When an execution error occurs, Cisco Unified CM automatically restores the message to the original content before applying additional error handling actions. If error handling specifies Rollback only, no further action is taken beyond rolling back to the original message before the normalization attempt. For the other possible Script Execution Error Recovery Actions, message rollback always occurs first, followed by the specified action, such as disabling the script, resetting the script automatically, or resetting the trunk automatically.
msgAddContentBody	This counter represents the number of times that the script added a content body to the message. If you are using the msg:addContentBody API in the script, this counter increases each time that the msg:addContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeader	This counter represents the number of times that the script added a SIP header to the message. If you are using the msg:addHeader API in the script, this counter increases each time that the msg:addHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header URI parameter to a SIP header in the message. If you are using the msg:addHeaderUriParameter API in the script, this counter increases each time that the msg:addHeaderUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.

Table 3 Cisco SIP Normalization (continued)

Display Name	Description
msgAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header value parameter to a SIP header in the message. If you are using the msg:addHeaderValueParameter API in the script, this counter increases each time that the msg:addHeaderValueParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgApplyNumberMask	This counter represents the number of times that the script applied a number mask to a SIP header in the message. If you are using the msg:applyNumberMask API in the script, this counter increases each time that the msg:applyNumberMask API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgBlock	This counter represents the number of times that the script blocked a message. If you are using the msg:block API in the script, this counter increases each time that the msg:block API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgConvertDiversionToHI	This counter represents the number of times that the script converted Diversion headers into History-Info headers in the message. If you are using the msg:convertDiversionToHI API in the script, this counter increases each time that the msg:convertDiversionToHI API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgConvertHIToDiversion	This counter represents the number of times that the script converted Diversion headers into History-Info headers in the message. If you are using the msg:convertDiversionToHI API in the script, this counter increases each time that the msg:convertDiversionToHI API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgModifyHeader	This counter represents the number of times that the script modified a SIP header in the message. If you are using the msg:modifyHeader API in the script, this counter increases each time that the msg:modifyHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveContentBody	This counter represents the number of times that the script removed a content body from the message. If you are using the msg:removeContentBody API in the script, this counter increases each time that the msg:removeContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeader	This counter represents the number of times that the script removed a SIP header from the message. If you are using the msg:removeHeader API in the script, this counter increases each time that the msg:removeHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeaderValue	This counter represents the number of times that the script removed a SIP header value from the message. If you are using the msg:removeHeaderValue API in the script, this counter increases each time that the msg:removeHeaderValue API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetRequestUri	This counter represents the number of times that the script modified the request URI in the message. If you are using the msg:setRequestUri API in the script, this counter increases each time that the msg:setRequestUri API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.

Table 3 Cisco SIP Normalization (continued)

Display Name	Description
msgSetResponseCode	This counter represents the number of times that the script modified the response code and/or response phrase in the message. If you are using the msg:setResponseCode API in the script, this counter increases each time that the msg:setResponseCode API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetSdp	This counter represents the number of times that the script set the SDP in the message. If you are using the msg:setSdp API in the script, this counter increases each time that the msg:setSdp API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddContentBody	This counter represents the number of times that the script added a content body to the PassThrough (pt) object. If you are using the pt:addContentBody API in the script, this counter increases each time that the pt:addContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeader	This counter represents the number of times that the script added a SIP header to the PassThrough (pt) object. If you are using the pt:addHeader API in the script, this counter increases each time that the pt:addHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header URI parameter to the PassThrough (pt) object. If you are using the pt:addHeaderUriParameter API in the script, this counter increases each time that the pt:addHeaderUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header value parameter to the PassThrough (pt) object. If you are using the pt:addHeaderValueParameter API in the script, this counter increases each time that the pt:addHeaderValueParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddRequestUriParameter	This counter represents the number of times that the script added a request URI parameter to the PassThrough (pt) object. If you are using the pt:addRequestUriParameter API in the script, this counter increases each time that the pt:addRequestUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ScriptActive	This counter indicates whether the script is currently active (running on the trunk). The following values display for the counter: • 0—Indicates that the script is closed (disabled). • 1—Indicates that the script is open and operational. To open the script that should be running on this trunk, perform the following actions: 1. Check for any alarms that might indicate why the script is not open. 2. Correct any errors. 3. Upload a new script if necessary. 4. Reset the trunk.

Table 3 Cisco SIP Normalization (continued)

Display Name	Description
ScriptClosed	This counter indicates the number of times that Cisco Unified Communications Manager has closed the script. When the script is closed, it is not enabled on this device. Cisco Unified CM closes the script under one of the following conditions: • The device was reset manually. • The device was reset automatically (due to an error). • The device was deleted. This count restarts when the SIP trunk is reset after a change to the script configuration and when Cisco Unified CM restarts.
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disabled the script. The values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified CM Administration determine whether the script is disabled. The script also gets disabled as a result of script error conditions that are encountered during loading and initialization. This counter provides a count from the most recent manual device reset that involved a script configuration change (a device reset alone does not restart the count; the script must also have changed before the reset occurs). This counter increments every time Cisco Unified CM automatically disables a script due to script errors. If the number in this counter is higher than expected, perform the following actions: • Check for SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Table 3 Cisco SIP Normalization (continued)

Display Name	Description
ScriptOpened	This counter indicates the number of times that the Cisco Unified CM attempted to open the script. For the a script to open, it must load into memory in Cisco Unified CM, initialize, and be operational. A number greater than one in this counter means that Cisco Unified CM has made more than one attempt to open the script on this SIP trunk, either for an expected reason or due to an error during loading or initialization. The error can occur due to execution errors or resource errors or invalid syntax in the script. Expect this counter to be greater than one if any of these counters increment: DeviceResetManually, DeviceResetAutomatically, or ScriptResetAutomatically. The DeviceResetManually counter increments when an expected event, such as a maintenance window on the SIP trunk, causes the script to close. If the number in this counter is high for an unexpected reason, perform the following actions: • Check for alarms, such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the SIP trunk resets after a script configuration change and when Cisco Unified CM restarts.
ScriptResetAutomatically	This counter indicates the number of times that the system automatically reset the script. The script resets based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified CM Administration. This counter specifies a count of the number of automatic script resets after the last manual device reset; this counter increments every time the Cisco Unified CM automatically resets a script due to script errors. If the number in this counter is higher than expected, perform the following actions: • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Serviceability - Alarms for Single Sign On and SmartCard Authentication

The following existing alarms are modified for Single Sign On and SmartCard Authentication:

- authFail, page 81
- authSuccess, page 82
- authLdapInactive, page 82

authFail

Failed to authenticate this user.

Cisco Unified Serviceability Alarm Definition Catalog
System/IMS

Severity
Warning (4)

Parameters
UserID(String)
Message(String)

Recommended Action
Determine correct credentials and retry.

authSuccess

Successfully authenticated this user.

Cisco Unified Serviceability Alarm Definition Catalog
System/IMS

Severity
Informational (6)

Parameters
UserID(String)

Recommended Action
None

authLdapInactive

Authentication failed because the user exists in the database and the system specifies LDAP authentication. A directory sync got performed in the immediate past (one day).

Cisco Unified Serviceability Alarm Definition Catalog
System/IMS

Severity
Warning (4)

Parameters
UserID(String)

Recommended Action
This user has yet to be removed from the database or the alarm will clear itself within 24 hours.

The following new alarms are generated for Single Sign On and SmartCard Authentication:

- LDAPServerUnreachable, page 83
- SSODisabled, page 83

- SSONullTicket, page 83
- SSOServerUnreachable, page 84
- SSOuserNotInDB, page 84

LDAPServerUnreachable

Authentication server could not be reached.

Cisco Unified Serviceability Alarm Definition Catalog
System/IMS

Severity
Warning

Parameters
Message(String)

Recommended Action
Check reachability to Authentication Server.

SSODisabled

Single Sign On (SSO) disabled on Cisco Unified CM.

Cisco Unified Serviceability Alarm Definition Catalog
System/IMS

Severity
Warning

Parameters
Message(String)

Recommended Action
Run CLI command to enable SSO.

SSONullTicket

A null ticket was passed.

Cisco Unified Serviceability Alarm Definition Catalog
System/IMS

Severity
Warning

Parameters
Message(String)

Recommended Action

Get non null ticket and retry.

SSOServerUnreachable

SSO server could not be reached.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning

Parameters

Message(String)

Recommended Action

Check reachability to SSO server.

SSOuserNotInDB

User not found in database.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Message(String)

Recommended Action

Perform sync manually or wait till next scheduled next sync.

Serviceability - Enhanced Reason Codes for Device De-Reg

Table 4 provides the reason codes that are added for EndPointTransientConnection alarm.

Table 4 Reason Codes for EndPoint TransientConnection Alarm

Reason Code	Description
maxDevRegExceeded	Maximum number of device registrations have been reached.
DeviceInitiatedReset	Indicates that the error was due to device initiated reset.
CallManagerReset	Indicates that the error was due to call manager reset.

Table 4 Reason Codes for EndPoint TransientConnection Alarm

Reason Code	Description
DirectoryNumberMismatch	Indicates mismatch between the directory number that the SIP device is trying to register with and the directory number configured in the Cisco Unified CM for the SIP device.
DatabaseTimeout	Cisco Unified CM requested device configuration data from the database but did not receive a response within 10 minutes.
RegistrationSequenceError	(SCCP only) A device requested configuration information from the Cisco Unified CM at an unexpected time. The Cisco Unified CM had not yet obtained the requested information. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error.
InvalidCapabilities	(SCCP only) The Cisco Unified CM detected an error in the media capabilities reported in the StationCapabilitiesRes message by the device during registration. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a protocol error.
CapabilityResponseTimeout	(SCCP only) The Cisco Unified CM timed out while waiting for the device to respond to a request to report its media capabilities. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops, and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify that the device is powered up and operating. Verify that network connectivity exists between the device and Cisco Unified CM, and verify that the CPU utilization is in the safe range.
SecurityMismatch	Unified CM detected a mismatch in the security settings of the device and/or the Cisco Unified CM. The following mismatches are detected: • The device established a secure connection, yet reported that it does not have the ability to do authenticated signaling. • The device did not establish a secure connection, but the security mode configured for the device indicates that it should have done so. • The device established a secure connection, but the security mode configured for the device indicates that it should not have done so
AutoRegisterDBError	Auto-registration of a device failed for one of the following reasons: • Auto-registration is not allowed for the device type. • An error occurred in the auto-registration stored procedure.
DBAccessError	Device registration failed because of an error that occurred while building the station registration profile. This usually indicates a synchronization problem with the database.
AutoRegisterDBConfigTimeout	(SCCP only) Unified CM timed out during auto-registration of a device. The registration profile of the device did not get inserted into the database in time. The device will automatically attempt to register again.

Table 4 Reason Codes for EndPoint TransientConnection Alarm

Reason Code	Description
DeviceTypeMismatch	The device type reported by the device does not match the device type configured on the Unified CM.
AddressingModeMismatch	(SCCP only) Cisco Unified CM detected an error related to the addressing mode configured for the device. One of the following errors was detected: • The device is configured to use only IPv4 addressing, but did not specify an IPv4 address. • The device is configured to use only IPv6 addressing, but did not specify an IPv6 address.

Table 5 provides the reason codes that are added for EndPointUnregistered alarm.

Table 5 Reason Codes for EndPointUnregistered alarm

Reason Code	Description
NoEntryInDatabase	Device not configured properly in the Cisco Unified CM database.
DatabaseConfigurationError	Device configuration error in the Cisco Unified CM database
DeviceNameUnresolveable	The Cisco Unified CM is unable to resolve the device name to an IP Address internally.
MaxDevRegExceeded	Maximum number of device registrations have been reached.
InitializationError	Indicates that an error occurred when the Cisco Unified CM tries to initialize the device.
PowerSavePlus	The device powered off as a result of the Power Save Plus feature that is enabled for this device. When the device powers off, it remains unregistered from Cisco Unified CM until the Phone On Time defined in the Product Specific Configuration for this device.
CallManagerForcedRestart	(SIP Only) The device did not respond to an Apply Config request and as a result, Unified CM sent a restart request to the device. The device may be offline due to a power outage or network problem. Confirm that the device is powered-up and that network connectivity exists between the device and Cisco Unified CM.
SourceIPAddrChanged	(SIP Only) The device has been unregistered because the IP address in the Contact header of the REGISTER message has changed. The device will be automatically reregistered. No action is necessary.
SourcePortChanged	(SIP Only) The device has been unregistered because the port number in the Contact header of the REGISTER message has changed. The device will be automatically re-registered. No action is necessary.
RegistrationSequenceError	A device requested configuration information from the Unified CM at an unexpected time. The Unified CM no longer had the requested information in memory.
InvalidCapabilities	(SCCP only) Cisco Unified CM detected an error in the updated media capabilities reported by the device. The device reported the capabilities in one of the StationUpdateCapabilities message variants.

Table 5 Reason Codes for EndPointUnregistered alarm

Reason Code	Description
FallbackInitiated	The device has initiated a fallback and will automatically reregister to a higher-priority Cisco Unified CM. No action is necessary.
DeviceSwitch	A second instance of an endpoint with the same device name has registered and assumed control. No action is necessary.

Serviceability - Session Manager Edition (SME)

Description

The Cisco Unified Communications Manager captures and logs all SIP message activities, which comprise the incoming and outgoing calls or sessions that pass through the Cisco Unified Communications Manager. The Cisco Unified Communications Manager stores the messages on a per-transaction basis in a new Call Log file, which can be downloaded through Real Time Monitoring Tool (RTMT) for post-processing activity.

RTMT users can search or trace the calls based on the following criteria:

- Calling Number/URI
- Called Number/URI
- Start Time
- Duration

RTMT downloads the Call Log file that includes the Start Time and Duration. The tool searches for the matching calls, lists the matching call records, and provides the SIP message Call Flow Diagram.

Before you Begin

Perform the following task:

- Use the enterprise parameter, Enable Call Trace Log, to enable or disable Call Tracing. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide*.
- The default value for maximum number of Call Trace log files specifies 2000 and the default value for maximum Call Trace log file size specifies 2 MB.

Procedure

Step 1 To display information on Session Trace, from the RTMT menus, choose **CallManager > Call Process > Session Trace**.

The Session Trace screen displays.

Step 2 Enter the search criteria and Click **Run**.

Note You can search calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. The search applies to the entire Unified CM cluster, not just the local node. If any node fails to collect the trace files, the system displays an error message in the bottom panel and pops up the message prompt to the user.

Click **Yes** to ignore the error and generate the table, based on the input.

Note In Calling Number/URI, Called Number/URI, you can use wild character "*" to match any number of characters. For example, a search for 123* fetches numbers like "123", "123456", "123*", "1234", etc.
If you want to search for numbers with a "*" in them, use "*". For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, and Termination Cause Code. The Termination Cause Code helps to identify the failure calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parenthesis followed by description.

Consider the following scenario:

- If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

Note If cause code description is missing or if you want more information on the Termination Cause Codes, refer the CDR cause codes in *Cisco Unified Call Details Records Administration Guide*.

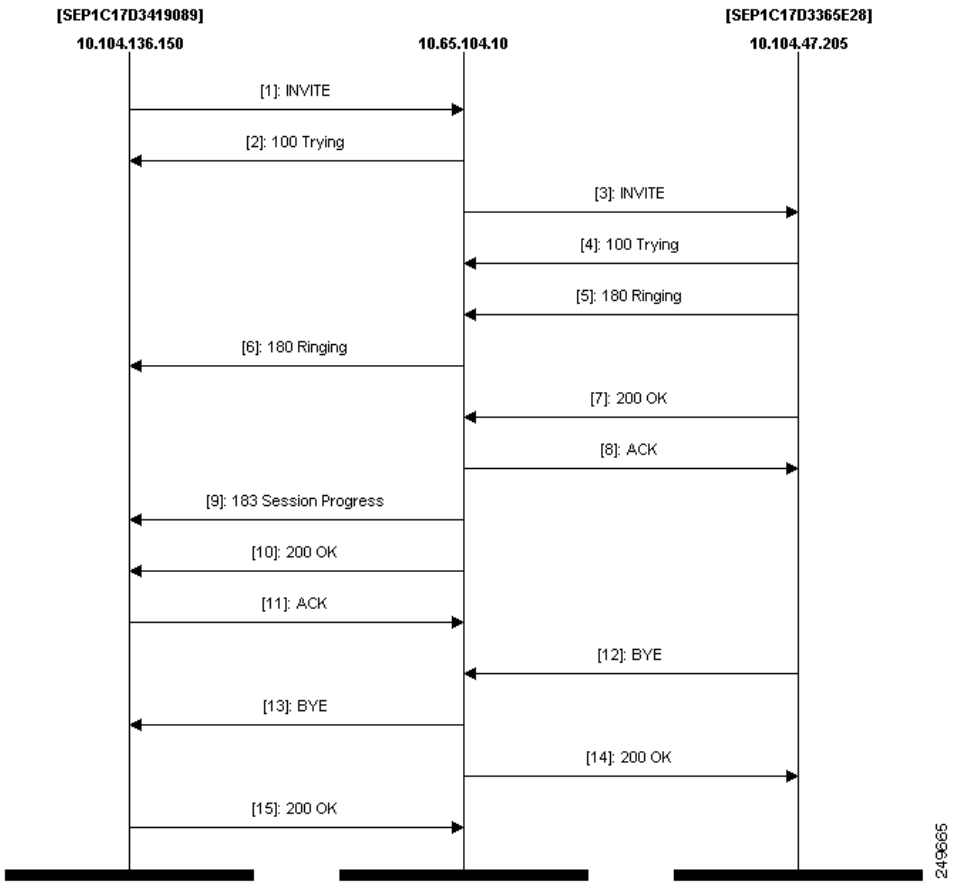
Step 3 Select a call (a row) to trace.

By default, **Include SIP Message** check box is selected to view the associated SIP protocol messages or call transactions.

Step 4 To generate the SIP Message Call Flow Diagram, click **Trace Call**. If you want to stop the generation of the session information, click **Cancel** on the progress window.

The Analyze Call Diagram window displays the corresponding SIP messages in the Call Flow Diagram.

Figure 1-1 Call Flow Diagram for Simple Call Scenario



Step 5 Click the tabs that you want to view. The following tabs are available:

- Call Flow Diagram—Displays the corresponding SIP messages in the Call Flow Diagram.
- Log File—Displays the entire log file.
- SIP Message—Appears only when the **Include SIP Message** check box is checked. Displays the actual SIP message that gets logged into the SDI log file.

Step 6 The following table lists the messages that display when you move your mouse on each SIP message in the Call Flow Diagram:

Displayed Messages	Description
Sender	Displays the IP address of the originating call.
SIP Call ID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or180 Ringing.
Receiver	Displays the IP address of the destination call.
Device Name	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.

Displayed Messages	Description
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

- Click the **See message in log file** link to view the subset of call logs that can be downloaded and analyzed.
- Click the **See SIP Message** link. A new **SIP Message** tab displays adjacent to the **Log File** tab. Click the **SIP message** tab to display the actual SIP message that gets logged into the SDI log file.

  To view the SIP messages that get logged into the SDI log file, do the following:

  – check the **Enable SIP Call Processing Trace** check box in the Trace Configuration window of Cisco Unified Serviceability (**Trace > Configuration**). See *Cisco Unified Serviceability Administration Guide* for more information.

  – set the trace level to any one of the following—State Transition, Significant, Arbitrary or Detailed.

Note You can view the **See SIP Message** link only when the **Include SIP Message** check box is checked.

Step 7 Click **Save.**

The call flow diagram gets saved as index.html in the specified folder along with the SIP messages. You can email the files to the Technical Assistance Center (TAC).

Note If the files are zipped, extract the zipped files to a local folder and open them to view the images.

You can do the following:

a. To view the online help, click **Help**.

b. To exit the Analyze Call Diagram screen, click **Close**.

c. To navigate to the previous page, click **Previous Messages**.

d. To navigate to the next page, click **Next Messages**.

Note **Previous Messages** or **Next Messages** is enabled only when the message size exceeds a threshold.

Call Log files

The Session Manager logs the call data in new log files. These new log files are located in the following folder: /var/log/active/cm/trace/ccm/calllogs/.

The Call Log name has the following file name pattern: calllogs_dddddddd.txt.gz.

The Call Logs include the following message types:

- Call Control—Writes call information at call setup, split, join and release.

```
Timestamp|MessageType (CC)|Operation (SETUP/SPLI/JOIN/RELEASE)|CI for one leg (aCI)|CI
for other leg (bCI)|calling DN|Orig Called DN|Final Called DN
```

- Device Layer—Writes metadata information that relates to message from or to the device.

```
Timestamp|MessageType (SIPL/SIPT)|My leg CI|Protocol(tcp/ucp)|Direction (IN/OUT)|local
ip|local port|device name|device ip|device port|Correlation id|Message Tag|SIP Call
ID|SIP method
```

Scenarios while Uninstalling RTMT

Consider the following scenarios, while uninstalling RTMT:

1. User saves the call flow diagram files in a folder (created by the user under **user.dir** directory)—All the files in **user.dir** are deleted except the newly created folder and the **user.dir** directory.
2. User saves the call flow diagram files in a folder (created during RTMT installation) under **user.dir** directory—All the files in **user.dir** are deleted including the **user.dir** directory.
3. User directly saves the call flow diagram files under **user.dir** directory—All the files in **user.dir** are deleted except the newly created files and the **user.dir** directory.
4. User saves the call flow diagram files in a folder which is outside **user.dir** directory—**user.dir** and its contents are removed. The folder created by the user is not deleted.

Limitations

The following limitations apply when the Call Flow Diagram gets generated:

- Search does not show incomplete calls.

  `Example:`

  When the user picks up the handset and hangs up without dialing the complete DN, it will not be listed in the search results.

- The Call Flow Diagram does not show some SIP messages in the following scenarios:
  - Conference calls involving more than three parties.
  - A call leg is used to invoke a feature alone.

  `Example`:

  Phone B and Phone C are in the same pickup group.

  1. User A calls Phone B.
  2. User C lifts up the Phone C handset.
  3. User C presses the PickUp softkey to pickup the call.

  SIP messages exchanged in Step 2 are not displayed in the Call Flow Diagram.

  In these cases, a RELEASE message is logged in the call logs without a corresponding SETUP message.

GUI Changes

Use the enterprise parameter, Enable Call Trace Log, to enable or disable the Call Tracing. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide*.

A new Session Trace window allows you to search for the matching calls, lists the matching call records, and provide the SIP message Call Flow Diagram. In RTMT, choose **CallManager > Call Process > Session Trace**.

Service Parameter and Enterprise Parameter Changes

A new enterprise parameter, Enable Call Trace Log, allows you to enable or disable the call tracing. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide*.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.5(1), you can use this feature.

Serviceability Considerations

You can enable call tracing by checking the Enable Call Trace Log checkbox on the Trace Configuration window in Cisco Unified Serviceability.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Default Settings for Alarm Configuration Settings

The default alarm configuration settings information is included in the *Cisco Unified Serviceability Administration Guide*.

Table 6 describes the default alarm configuration settings.

Table 6 Default Alarm Configuration Settings

	Local Syslogs	Remote Syslogs	SDI Trace	SDL Trace
Enable Alarm	Checked	Unchecked	Checked	Checked
Alarm Event Level	Error	Disabled	Error	Error

New Cisco Unity Connection Alerts

The following new alerts are added for Cisco Unity Connection:

- DiskConsumptionCloseToCapacityThreshold, page 93
- DiskConsumptionExceedsCapacityThreshold, page 93

DiskConsumptionCloseToCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server reaches ten percent below the percentage limit specified on the **System Settings > Advanced > Disk Capacity** in Cisco Unity Connection Administration. For example, with a capacity threshold limit of 95 percent, the alert is triggered when usage reaches at least 85 percent.

Default Configuration

Table 7 lists the default configuration for the DiskConsumptionCloseToCapacityThreshold RTMT Alert.

Table 7 Default Configuration for the DiskConsumptionCloseToCapacityThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionCloseToCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionExceedsCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server meets or exceeds the percentage limit specified on the **System Settings > Advanced > Disk Capacity** in Cisco Unity Connection Administration.

Default Configuration

Table 8 Default Configuration for the DiskConsumptionExceedsCapacityThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionExceedsCapacityThreshold event generated
Duration	Trigger alert immediately

Table 8 Default Configuration for the DiskConsumptionExceedsCapacityThreshold RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

New CDR Field for Hunt List Support

Table 9 describes the new CDR field for the hunt list support.

Table 9 New CDR Field for Hunt Lists

Name	Range of Values	Description
calledPartyPatternUsage	Positive Integer	This field indicates the pattern of the called party. Default value is 5 (PATTERN_ROUTE). • If the huntPilotDN is populated, use the field value of huntPilotDN as the hunt pilot. • If the huntPilotDN is not available, check the pattern usage (7 = PATTERN_HUNT_PILOT) in the CDR table to identify the call type. If this call is a hunt list call, use the finalCalledPartyNumber as the huntPilotDN.

SNMP MIBs

The following TEXTUAL-CONVENTIONs are updated for MIB objects:

- CcmDevRegFailCauseCode
- CcmDevUnregCauseCode

  CcmDevRegFailCauseCode ::= TEXTUAL-CONVENTION

  STATUS current

  DESCRIPTION

  This syntax is used as means of identifying the reasons for a device registration failure. The scope of this enumeration can expand to comply with RFC 2578.

  noError: No Error

  unknown: Unknown error cause

  noEntryInDatabase: Device not configured properly in the Cisco Unified CM database

  databaseConfigurationError: Device configuration error in the Cisco Unified CM database

deviceNameUnresolveable: The Cisco Unified CM is unable to resolve the device name to an IP Address internally

maxDevRegExceeded: Maximum number of device registrations have been reached

connectivityError: Cisco Unified CM is unable to establish communication with the device during registration

initializationError: Indicates an error occurred when the Cisco Unified CM tries to initialize the device

deviceInitiatedReset: Indicates that the error was due to device initiated reset

callManagerReset: Indicates that the error was due to call manager reset.

authenticationError: Indicates mismatch between configured authentication mode and the authentication mode that the device is using to connect to the Cisco Unified CM.

invalidX509NameInCertificate: Indicates mismatch between the peer X.509 certificate subject name and what is configured for the device.

invalidTLSCipher: Indicates Cipher mismatch during TLS handshake process.

directoryNumberMismatch: Indicates mismatch between the directory number that the SIP device is trying to register with and the directory number configured in the Cisco Unified CM for the SIP device.

malformedRegisterMsg: Indicates that SIP device attempted to register with Cisco Unified CM, but the REGISTER message contained formatting errors.

protocolMismatch: The protocol of the device (SIP or SCCP) does not match the configured protocol in Cisco Unified CM.

deviceNotActive: The device has not been activated.

authenticatedDeviceAlreadyExists: A device with the same name is already registered with Cisco Unified CM.

obsoleteProtocolVersion: The SCCP device registered with an obsolete protocol version.

databaseTimeout: Cisco Unified CM requested device configuration data from the database but did not receive a response within 10 minutes.

registrationSequenceError: (SCCP only) A device requested configuration information from the Cisco Unified CM at an unexpected time. The Cisco Unified CM had not yet obtained the requested information. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error.

invalidCapabilities: (SCCP only) The Cisco Unified CM detected an error in the media capabilities reported in the StationCapabilitiesRes message by the device during registration. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a protocol error.

capabilityResponseTimeout: (SCCP only) The Cisco Unified CM timed out while waiting for the device to respond to a request to report its media capabilities. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops, and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify that the device is powered up and operating. Verify that network connectivity exists between the device and Cisco Unified CM, and verify that the CPU utilization is in the safe range.

securityMismatch: The Cisco Unified CM detected a mismatch in the security settings of the device and/or the Cisco Unified CM. The mismatches that can be detected are:

- The device established a secure connection, yet reported that it does not have the ability to do authenticated signaling.
- The device did not establish a secure connection, but the security mode configured for the device indicates that it should have done so.
- The device established a secure connection, but the security mode configured for the device indicates that it should not have done so.

autoRegisterDBError—Auto-registration of a device failed for one of the following reasons:

- Auto-registration is not allowed for the device type.
- An error occurred while adding the auto-registering device to the database (stored procedure).

dbAccessError: Device registration failed because of an error that occurred while building the station registration profile. This usually indicates a synchronization problem with the database.

autoRegisterDBConfigTimeout: (SCCP only) The Cisco Unified CM timed out during auto-registration of a device. The registration profile of the device did not get inserted into the database in time. The device will automatically attempt to register again.

deviceTypeMismatch: The device type reported by the device does not match the device type configured on the Cisco Unified CM.

addressingModeMismatch: (SCCP only) The Cisco Unified CM detected an error related to the addressing mode configured for the device. One of the following errors were detected:

- The device is configured to use only IPv4 addressing, but did not specify an IPv4 address.
- The device is configured to use only IPv6 addressing, but did not specify an IPv6 address.

SYNTAX INTEGER {

noError(0),

unknown(1),

noEntryInDatabase(2),

databaseConfigurationError(3),

deviceNameUnresolveable(4),

maxDevRegExceeded(5),

connectivityError(6),

initializationError(7),

deviceInitiatedReset(8),

callManagerReset(9),

authenticationError(10),

invalidX509NameInCertificate(11),

invalidTLSCipher(12),

directoryNumberMismatch(13),

malformedRegisterMsg(14),

protocolMismatch(15),

deviceNotActive(16),

authenticatedDeviceAlreadyExists(17),

obsoleteProtocolVersion(18),

databaseTimeout(23),

registrationSequenceError(25),

invalidCapabilities(26),

capabilityResponseTimeout(27),

securityMismatch(28),

autoRegisterDBError(29),

dbAccessError(30),

autoRegisterDBConfigTimeout(31),

deviceTypeMismatch(32),

addressingModeMismatch(33)

}

CcmDevUnregCauseCode ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

This syntax is used as means of identifying the reasons for a device getting unregistered. The scope of this enumeration can expand to comply with RFC 2578.

noError: No Error

unknown: Unknown error cause

noEntryInDatabase: Device not configured properly in the Cisco Unified CM database

databaseConfigurationError: Device configuration error in the Cisco Unified CM database

deviceNameUnresolveable: The Cisco Unified CM is unable to resolve the device name to an IP Address internally

maxDevRegExceeded: Maximum number of device registrations have been reached

connectivityError: Cisco Unified CM is unable to establish communication with the device during registration

initializationError: Indicates that an error occurred when the Cisco Unified CM tries to initialize the device

deviceInitiatedReset: Indicates that the error was due to device initiated reset

callManagerReset: Indicates that the error was due to Cisco Unified CM reset.

deviceUnregistered: DeviceUnregistered.

malformedRegisterMsg: Indicates that SIP device attempted to register with Cisco Unified CM, but the REGISTER message contained formatting errors.

sccpDeviceThrottling: The indicated SCCP device exceeded the maximum number of events allowed per-SCCP device.

keepAliveTimeout: A KeepAlive message was not received. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops, packet corruption and Cisco Unified CM node experiencing high CPU usage.

configurationMismatch: The configuration on the SIP device does not match the configuration in Cisco Unified CM.

callManagerRestart: A device restart was initiated from Cisco Unified CM Administration, either due to an explicit command from an administrator or due to a configuration change such as adding, deleting or changing a directory number associated with the device.

duplicateRegistration: Cisco Unified CM detected that the device attempted to register to two nodes at the same time. Cisco Unified CM initiated a restart to the phone to force it to re-home to a single node.

callManagerApplyConfig: Cisco Unified CM configuration is changed.

deviceNoResponse: Device is not responding Service Control Notify from Cisco Unified CM.

emLoginLogout: The device has been unregistered due to an Extension Mobility login or logout.

emccLoginLogout: The device has been unregistered due to an Extension Mobility Cross Cluster login or logout.

powerSavePlus: The device powered off as a result of the Power Save Plus feature that is enabled for this device. When the device powers off, it remains unregistered from Cisco Unified CM until the Phone On Time defined in the Product Specific Configuration for this device.

callManagerForcedRestart: (SIP Only) The device did not respond to an Apply Config request and as a result, Cisco Unified CM had sent a restart request to the device. The device may be offline due to a power outage or network problem. Confirm that the device is powered-up and that network connectivity exists between the device and Cisco Unified CM.

sourceIPAddrChanged: (SIP Only) The device has been unregistered because the IP address in the Contact header of the REGISTER message has changed. The device will be automatically reregistered. No action is necessary.

sourcePortChanged: (SIP Only) The device has been unregistered because the port number in the Contact header of the REGISTER message has changed. The device will be automatically reregistered. No action is necessary.

registrationSequenceError: A device requested configuration information from the Cisco Unified CM at an unexpected time. The Cisco Unified CM no longer had the requested information in memory.

invalidCapabilities: (SCCP only) The Cisco Unified CM detected an error in the updated media capabilities reported by the device. The device reported the capabilities in one of the StationUpdateCapabilities message variants.

fallbackInitiated: The device has initiated a fallback and will automatically reregister to a higher-priority Cisco Unified CM. No action is necessary.

deviceSwitch: A second instance of an endpoint with the same device name has registered and assumed control. No action is necessary.

SYNTAX INTEGER {

noError(0),

unknown(1),

noEntryInDatabase(2),

databaseConfigurationError(3),

deviceNameUnresolveable(4),

maxDevRegExceeded(5),

connectivityError(6),

initializationError(7),

deviceInitiatedReset(8),
callManagerReset(9),
deviceUnregistered(10),
malformedRegisterMsg(11),
sccpDeviceThrottling(12),
keepAliveTimeout(13),
configurationMismatch(14),
callManagerRestart(15),
duplicateRegistration(16),
callManagerApplyConfig(17),
deviceNoResponse(18),
emLoginLogout(19),
emccLoginLogout(20),
energywisePowerSavePlus(21),
callManagerForcedRestart(22),
sourceIPAddrChanged(23),
sourcePortChanged(24),
registrationSequenceError(25),
invalidCapabilities(26),
fallbackInitiated(28),
deviceSwitch(29)

Logging On to CAR

Before you log on to CAR, perform one of the following tasks:

- For CAR system administrators only—From Cisco Unified Serviceability, choose **Tools > CDR Analysis and Reporting**.
- For CAR users or administrators—From the web browser, enter

  https://<Server-ip/name>:8443/car/

Configuring the Trunk

Tip Configure the trunks in CAR for existing Cisco Unified Communications Manager system trunks. After you add trunks to Cisco Unified Communications Manager Administration, configure the new trunks in CAR. When trunks are deleted from the Cisco Unified Communications Manager system, the system automatically removes the trunks (and any configuration settings that you specified) from CAR.

CAR uses the area code information to determine whether calls are local or long distance. You must provide the Number of Ports information for each trunk to enable CAR to generate the Utilization reports.

This section describes how to configure trunks in CAR.

Procedure

Step 1 Choose **System > System Parameters > Trunk Configuration**.

The Trunk Configuration window displays.

Note If you have not configured trunks in Cisco Unified Communications Manager Administration, a message displays that indicates that you have not configured trunks for the system.

Note CAR uses the area code information to determine whether calls are local or long distance. For 8.5(1) release, the area code is not updated for all the trunks.

Step 2 In the Max No. of Ports field, enter the number of ports for each trunk that you want to configure. The maximum number of ports range from 1 to 1000.

Note CAR uses the values that were provided for the trunk when it was added in Cisco Unified Communications Manager Administration. Therefore, some trunks will already have a zero for maximum number of ports, depending on the details that were specified when the trunk was added in Cisco Unified Communications Manager Administration. CAR does not accept zero as a value for the maximum number of ports; you may be prompted to change the maximum number of ports for all trunks with a value of zero.

Step 3 To make the changes, click the **Update** button.

You can run reports in CAR on any or all of the configured trunks.

Configuring Trunk Utilization Reports

Only CAR administrators generate the Trunk Utilization report. This report calculates the utilization reports for devices based on the duration of calls that passed through the devices.

You can generate this report on an hourly, daily, or monthly basis. The system calculates the utilization of a trunk for each hour in the selected date range. For example, the system calculates the utilization of a trunk between 11hrs-12hrs, using the formula, (Sum of the duration of calls that used the trunk in that hour / (total seconds in an hour * maximum number of ports in a trunk * number of days between the fromDate and toDate selected) * 100).

Similarly, to get the utilization for each day in a week, the system calculates the utilization using the formula, ((sum of the duration of calls that used the trunk in a day) / (total seconds in each day * number of each day between the fromDate and toDate selected * maximum number of ports in a trunk) * 100).

In the case of monthly utilization reports, the system calculates the utilization for each day in a month, using the formula, ((sum of the duration of calls that used the trunk in a day) / (total seconds in each day * number of each day between the fromDate and toDate selected * maximum number of ports in a trunk) * 100).

Reports generate for each trunk that is chosen.

For calculation of the trunk utilization, the system uses the port numbers from the CAR Trunk Configuration window. To find this window, choose **System > System Parameters > Trunk Configuration**. You cannot take port details for H.323 trunks from the Cisco Unified Communications Manager database because the H.323 port number always equals zero in the database. The user must update H.323 trunk ports information in the CAR Trunk Configuration window.

Be aware that the only port detail information that is taken from the CAR Trunk Configuration window is only for those trunks that do not have port details that are available or that show zero in the Cisco Unified Communications Manager database.

This section describes how to generate, view, or mail Trunk Utilization reports.

Procedure

Step 1 Choose **Device Reports > Trunk > Utilization**.

The Trunk Utilization window displays.

Step 2 In the Generate Reports field, choose a time as described in Table 10.

Table 10 Generate Report Fields

Parameter	Description
Hour of Day	Displays the cumulative utilization for each hour in a 24-hour period for the period that you specify in Step 7.
Day of Week	Displays the cumulative utilization for the days of the week that occur within the period that you specify in Step 7.
Day of Month	Displays the cumulative utilization for the days of the month that occur within the period that you specify in Step 7.

Note The Trunk Utilization report is not generated automatically.

Step 3 To display the list of trunks that you can include in the report in the List of Trunks box, perform one of the following tasks:

- To display all trunks in the List of Trunks box, click **Trunk Types** in the column on the left side of the window.
- To display trunks for a particular trunk type in the List of Trunks box, click the icon next to **Trunk Types** in the column on the left side of the window. The tree structure expands, and a list of trunk types displays. Choose a trunk type from the list, and the trunk name displays in the List of Trunks box.

Note The List of Trunks box will list up to 200 trunks that are configured for the chosen trunk type.

Note You can generate the trunk utilization reports for route groups, route lists, and route patterns that are connected through trunks.

Step 4 Choose a trunk type from the list.

The trunk name displays in the List of Trunks box.

Note The List of Trunks box displays up to 200 trunks that are configured for the chosen trunk type.

Step 5 In the List of Trunks box, choose the trunks that you want to include in the report.

Note You can generate a report for up to five trunks at a time.

Step 6 To move the chosen trunk to the list of Selected Trunks box, click the down arrow.

The trunk(s) that you chose displays in the Selected Trunks box.

Step 7 If you chose Generate New Report, enter the date range of the period for which you want to see call information.

Note Ensure the date and time range does not exceed one month.

Step 8 If you want the report in CSV format, choose **CSV** (comma separated value) in the Report Format area. If you want the report in PDF format, choose **PDF** (portable document format) in the Report Format area.

Step 9 Click the **View Report** button.

The report displays**.**

Step 10 If you want to mail the report, click the **Send Report** button.

Cisco Dialed Number Analyzer Server

The Cisco Dialed Number Analyzer Server service along with the Cisco Dialed Number Analyzer service supports Cisco Unified Communications Manager Dialed Number Analyzer. This service needs to be activated only on the node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

This service can be activated by choosing **Tools > Service Activation** and choosing **Tools > Dialed Number Analyzer Server**, from the Serviceability UI.

Unified CM clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

In a Cisco Unified Communications Manager Business Edition 5000 system, this service supports Cisco Unified Communications Manager only.

The following states the recommendation for the newly added service:

Service/ Servlet	Activation Recommendations
Cisco Dialed Number Analyzer Server	If you have more than one node in the cluster, activate this service on one node that is dedicated specifically for the Cisco Dialed Number Analyzer service.